

**ÜBER INVARIANTEN
SEPARABLER GALOISERWEITERUNGEN
KOMMUTATIVER RINGE**

Dissertation
zur Erlangung des akademischen Grades
eines Doktors der Naturwissenschaften
der Fakultät für Mathematik
der Ludwig-Maximilians-Universität München

vorgelegt von

Rudolf Hagenmüller
aus Krumbach

eingereicht im Mai 1979



Digitized by the Internet Archive
in 2026

**ÜBER INVARIANTEN
SEPARABLER GALOISERWEITERUNGEN
KOMMUTATIVER RINGE**

Dissertation
zur Erlangung des akademischen Grades
eines Doktors der Naturwissenschaften
der Fakultät für Mathematik
der Ludwig-Maximilians-Universität München

vorgelegt von

Rudolf Hagenmüller
aus Krumbach

eingereicht im Mai 1979



1. Berichterstatter : Prof. Dr. B. Pareigis
 2. Berichterstatter : Prof. Dr. H.-J. Schneider
- Tag der mündlichen Prüfung : 20. Juli 1979

INHALT

Einleitung	1
Kapitel 1 Modulstrukturen von Galoisweiterungen	15
eines kommutativen Ringes der Serre-Dimension 1	
§0 Einige Begriffe und Bezeichnungen	15
§1 Determinanten von Galoisweiterungen	18
§2 Der Charakter "Signatur"	28
§3 Diskriminanten von Galoisweiterungen	32
§4 Modulstrukturen von Galoisweiterungen	37
§5 Invarianten abelscher Galoisweiterungen	44
§6 Modulstrukturen von Galoisweiterungen mit zyklischen Galoisgruppen von 2-Potenz-Ordnung	49
Kapitel 2 Kohomologische Beschreibungen der Invarianten von Galoisweiterungen	58
§1 Verzerrte Formen	59
§2 Der Hauptsatz der Theorie der verzerrten Formen	73
§3 Beschreibung der Ecken des Invarianten- Diagrammes mit Amitsurscher Kohomologie	85
§4 Beschreibung der Pfeile des Invarianten- Diagrammes mit Amitsurscher Kohomologie	94
§5 Beschreibung des Invarianten-Diagrammes mit Čechscher Kohomologie	108

Kapitel 3	Die Gruppe der freien quadratischen Erweiterungen eines Ringes, in dem 2 ein Nicht-Nullteiler ist	119
§1	Das Invarianten-Diagramm im Fall quadratischer Erweiterungen	121
§2	Die Gruppe der freien quadratischen Erweiterungen	134
§3	Das Diagramm der exakten Kohomologiefolgen	151
§4	Diskriminanten und Picard-Invarianten freier quadratischer Erweiterungen	161
Anhang	Eine exakte Folge von C. Small	176
Kapitel 4	Freie quadratische Erweiterungen von Ordnungen in quadratischen Zahlkörpern	184
§0	Grundlagen und Bezeichnungen	184
§1	Die Gruppe der freien quadratischen Erweiterungen von A_q^d	187
§2	Die Gruppe der quadratischen Erweiterungen mit Normalbasis von A_q^d	208
Anhang	Bemerkungen zu Thérond [41]	217
Literatur		224

EINLEITUNG

Die vorliegende Arbeit beschäftigt sich mit Galois-
weiterungen im Sinn der von Auslander, Goldman [3] und
Chase, Harrison, Rosenberg [12, 13, 26] begründeten
separablen Galois-theorie kommutativer Ringe.

Der Picard-Invariante abelscher Galois-
weiterungen werden zwei weitere Invarianten zur Seite gestellt. Dann werden
die Eigenschaften des Invariantentripels untersucht. Als
Anwendungen ergeben sich Aussagen über die Modulstrukturen
von Galois-
weiterungen und über die Gruppen der freien
quadratischen Erweiterungen.

Doch schildern wir zunächst, aus welchen Fragestellungen
sich diese Arbeit entwickelte.

Ist G eine endliche abelsche Gruppe, so bilden die Iso-
morphieklassen der G - Galois-
weiterungen $^+$) eines
kommutativen Ringes R eine abelsche Gruppe $\text{Gal}(R, G)$.
 G - Galois-
weiterungen sind als Moduln über dem Gruppen-
ring $R[G]$ endlich erzeugt projektiv vom Rang 1 [35],
und die Zuordnung $\text{Gal}(R, G) \rightarrow \text{Pic}(R[G])$ respektiert
die Gruppenstrukturen [23]. Childs und Magid nannten sie
"Picard-Invariante" [16]. Ihr Kern besteht genau aus den

$^+$) Damit meinen wir Galois-
weiterungen mit Galoisgruppe G .

Isomorphieklassen von Galoiserweiterungen mit Normalbasis.

Für quadratische Erweiterungen werden in der Literatur neben der Picard-Invariante noch zwei weitere "Invarianten" betrachtet. Sie kommen auf folgende Weise zustande: Ist $R \hookrightarrow A$ eine quadratische Erweiterung, so ist der Spurhomomorphismus $\text{tr}_R^A : A \rightarrow R$ surjektiv; sein Kern ist deshalb ein invertierbarer R -Modul, und die Multiplikation induziert auf ihm eine nicht-ausgeartete Bilinearform. Die Zuordnungen $[A] \mapsto [\text{Ke}(\text{tr}_R^A)]$, $[A] \mapsto [\text{Ke}(\text{tr}_R^A), \text{mult}]$ sind Homomorphismen in die Picardgruppe von R bzw. in die Gruppe der R -Diskriminantenmoduln (vgl. [32, 36, 38]).

Diese "Invarianten" sind deshalb von Interesse, weil durch $[\text{Ke}(\text{tr}_R^A)] \in \text{Pic}(R)$ die R -Modulstruktur von A bis auf Isomorphie eindeutig bestimmt ist. Insbesondere besteht der Kern der einen genau aus den Klassen quadratischer Erweiterungen, welche als R -Moduln frei sind.

Überhaupt sind die quadratischen Erweiterungen in der Literatur sehr viel intensiver untersucht, als die übrigen Galoiserweiterungen. Das liegt einesteiis daran, daß sie in der Theorie der quadratischen Formen eine Rolle spielen. Daher rührt zum Beispiel bei folgenden Publikationen das Interesse an quadratischen Erweiterungen:

[4, 5, 27, 31, 32, 33, 36, 37]. Ein anderer Grund für die Sonderrolle der quadratischen Erweiterungen ist darin zu sehen, daß sich in diesem Fall viele Überlegungen stark vereinfachen. Nehmen wir zum Beispiel diejenigen Erweiterungen, welche als Moduln über dem Grundring frei sind.

Freie quadratische Erweiterungen sind von der Form $R[x] / (x^2 - ax - b)$ mit einem Paar (a, b) von Ringelementen, für welches $a^2 + 4b$ invertierbar ist [28]. Der Isomorphie von Erweiterungen entspricht eine Äquivalenzrelation auf der Menge dieser Paare. So gewinnt man eine Beschreibung der Gruppe der freien quadratischen Erweiterungen. Diese Gruppe sei im folgenden mit $\mathcal{F}(R)$ bezeichnet. Sie ist abelsch und hat den Exponent 2 [38]. Es genügt also ihre Dimension über dem Körper $GF(2)$ zu bestimmen, um sie bis auf Isomorphie zu kennen. Aber es zeigt sich, daß es im allgemeinen nicht leicht ist, zu einem vorgegebenen Ring diese $GF(2)$ -Dimension zu finden.

Der erste Versuch, dabei über die Betrachtung trivialer Fälle und vereinzelter Beispiele hinauszukommen, stammt von Thérond [41]. Er bestimmt die Gruppen der freien quadratischen Erweiterungen für die Hauptordnungen in reell-quadratischen Zahlkörpern. Doch unterlaufen ihm dabei mehrere schwere Fehler. Glücklicherweise heben sie sich teilweise gegenseitig auf, so daß die Ergebnisse nicht völlig falsch sind (vgl. Anhang zu Kapitel 4).

Dies war der Anstoß zur vorliegenden Arbeit. Théronds Ergebnisse sollten überprüft werden. Wollte man die Klasse der betrachteten Ringe nicht unnötig einschränken, so hieß das: Für die Ordnungen in quadratischen Zahlkörpern war die Gruppe $\mathcal{F}$ zu bestimmen.

Aus Théronds Arbeit war bereits bekannt, daß dazu der von Kitamura [28] eingeführte Homomorphismus

$$D : \mathcal{F}(R) \rightarrow \frac{U(R)}{U^2(R)}$$

ein geeignetes Hilfsmittel war. Für Ordnungen in quadratischen Zahlkörpern ist die Struktur der Einheitengruppe wohlbekannt [8]. Mit etwas Mühe lassen sich damit die $GF(2)$ - Dimensionen von $Ke(D)$ und $Bi(D)$ bestimmen.

Bei der Suche nach "allgemeinen Aussagen", welche hinter den Ergebnissen dieser Beispiele stecken, entstand ein weiterer Teil dieser Arbeit. In ihm wird mit kohomologischen Methoden gearbeitet. Die Invarianten quadratischer Erweiterungen lassen sich nämlich mit Čech-Kohomologie beschreiben. Für Ringe R^+ , in denen 2 ein Nicht-Nullteiler ist, sind sie Glieder langer exakter Kohomologiefolgen. Die langen exakten Folgen fügen sich zu einem "großen" Diagramm, aus dem sich eine siebengliedrige

⁺) In dieser Arbeit sind Ringe stets assoziativ, unitär und kommutativ.

exakte Folge gewinnen läßt, in deren Mitte Kitamuras D steht. Diese exakte Folge erweist sich als der gesuchte "abstrakte Hintergrund": die wichtigsten Hilfsätze des Beispielteils lassen sich daraus ableiten.

Als unerwartetes Nebenergebnis der kohomologischen Betrachtungen wurde eine Möglichkeit sichtbar, wie die Invarianten mit Werten in $\text{Pic}(R)$ und $\text{Dis}(R)$ für beliebige Galoiserweiterungen zu bilden wären. Diese verallgemeinerten Invarianten erwiesen sich als ein sehr brauchbares Instrument, um die Modulstrukturen von Galoiserweiterungen über dem Grundring zu untersuchen - vorausgesetzt der Grundring hatte Serre-Dimension 1 ⁺) .

Die Ergebnisse über die Modulstrukturen von Galoiserweiterungen haben mit den Ergebnissen über die Gruppen der freien quadratischen Erweiterungen von ihrem Inhalt her nichts zu tun. Wenn ich sie trotzdem gemeinsam vorlege, so geschieht dies deshalb, weil ich das hier Präsentierte infolge der Natürlichkeit seines Entstehens als Einheit empfinde. Diese Empfindung läßt sich

⁺) Damit meinen wir einen kommutativen Ring, über dem jeder endlich erzeugte projektive Modul konstanten Ranges in eine direkte Summe aus einem freien und einem invertierbaren Modul zerfällt.

durch die Beobachtung objektivieren, daß all die geschilderten Ergebnisse auf Eigenschaften der "Invarianten von Galois-erweiterungen" beruhen.

Es folgt nun ein Überblick über Aufbau und Inhalt der Arbeit.

In Kapitel 1 werden zunächst die beiden neuen Invarianten eingeführt. Dies basiert auf folgender Überlegung: Ist G eine endliche Gruppe der Ordnung n , so ist eine G -Galoisererweiterung A als R -Modul endlich erzeugt projektiv und hat konstanten Rang n [12]. Die n -te äußere Potenz $\bigwedge_R^n(A)$ ist daher ein invertierbarer R -Modul.

Die Abbildung $\det_R^G : \text{Gal}(R, G) \ni [A] \mapsto [\bigwedge_R^n(A)] \in \text{Pic}(R)$ nennen wir "Determinante". (Für nicht-abelsches G betrachten wir $\text{Gal}(R, G)$ nur als Menge.) Die andere Invariante, die "Diskriminante", ist eine Abbildung $\text{dis}_R^G : \text{Gal}(R, G) \longrightarrow \text{Dis}(R)$. Ist R ein Ring der Serre-Dimension 1, so garantieren Eigenschaften der äußeren Potenzen, daß die R -Modulstruktur von A durch $\det_R^G([A])$ bis auf Isomorphie eindeutig bestimmt ist.

Solange die Determinante jedoch nur in dieser abstrakten Form vorliegt, kann man sie kaum als brauchbares Instrument bezeichnen. Bisher würde man beispielsweise nicht

vermuten, daß $\det_R^G([A])$ von der Gruppenstruktur auf G abhängt. Der entscheidende Schritt von der formalen Definition zur aussagekräftigen Invariante wird durch folgende Beobachtung vollzogen: $\bigwedge_R^n(A)$ ist isomorph zum Fixuntermodul $A^{\text{sign}} = \{x \in A \mid \forall g \in G : g(x) = \text{sign}(g) x\}$. Dabei ist $\text{sign}(g)$ das Vorzeichen der Permutation, welcher g bei der regulären Darstellung entspricht.

Über die Modulstrukturen von Galoisweiterungen eines Ringes R der Serre-Dimension 1 können wir damit beweisen: Galoisweiterungen, deren Galoisgruppe von ungerader Ordnung ist oder deren Galoisgruppe nichtzyklische 2-Sylowuntergruppen besitzt, sind als R -Moduln frei. Besitzt G eine zyklische 2-Sylowuntergruppe $H \neq 0$, so treten bei G -Galoisweiterungen bis auf freie direkte Summanden dieselben R -Modulstrukturen auf wie bei H -Galoisweiterungen (Theorem 1.26.).

Die R -Modulstrukturen von Galoisweiterungen über R werden im wesentlichen durch folgende Kette abelscher Gruppen vom Exponent 2 beschrieben $\text{Bi}(\det_R^{C_2}) \supseteq \text{Bi}(\det_R^{C_4}) \supseteq \dots \supseteq \text{Bi}(\det_R^{C_{2^a}}) \supseteq \dots$ (Satz 1.44.).

Nebenbei sei bemerkt, daß die quadratischen Erweiterungen also auch hier wieder eine Sonderstellung einnehmen.

In der allgemeinen Galoistheorie war über die Modulstrukturen von Galoiserweiterungen über dem Grundring bisher kaum etwas bekannt. Für quadratische Erweiterungen wurde das Problem von C. Small [38] gelöst. Unter sehr speziellen Voraussetzungen erzielte auch Childs [14] einige Ergebnisse; doch handelt es sich dabei im Grunde nicht um Eigenschaften von Galoiserweiterungen, sondern um Konsequenzen aus Eigenschaften des Gruppenringes.

Doch in der algebraischen Zahlentheorie ist eine entsprechende Fragestellung seit langem geläufig: Ist $K \hookrightarrow L$ eine endliche Galoiserweiterung algebraischer Zahlkörper, und ist $R \hookrightarrow A$ die Erweiterung der zugehörigen Ringe ganzer algebraischer Zahlen, so beschreibt Fröhlichs Idéle-Diskriminante $\mathcal{S}^{(L/K)}$ die R -Modulstruktur von A (vgl. [19, 20, 21, 22]). Falls die Galoiserweiterung $K \hookrightarrow L$ unverzweigt ist, so ist bekanntlich $R \hookrightarrow A$ eine Galoiserweiterung mit derselben Galoisgruppe [12]. In diesem Fall wird also die R -Modulstruktur von A sowohl durch unsere Determinante als auch durch Fröhlichs Idéle-Diskriminante beschrieben.

Überraschenderweise findet man aber in der Literatur selbst in diesem Spezialfall nur folgende Teilaussage

unseres Theorems: Ist die Ordnung der Galoisgruppe ungerade, so besitzt $R \hookrightarrow A$ eine relative Ganzheitsbasis ([19] Theorem 4.3.). Wie mir Fröhlich im Juli 78 bei einem Gespräch in Oberwolfach mitteilte, hatte er die anderen Teile des Theorems nicht bemerkt. Bis dahin schienen sie auch nicht bekannt zu sein. Während der Niederschrift dieser Arbeit publizierte dann Maurer [30] den entscheidenden Hilfssatz, um mit Fröhlichs Methoden im genannten Spezialfall einen weiteren Teil unseres Theorems zu beweisen: Hat die Galoisgruppe gerade Ordnung und nicht-zyklische 2-Sylow-untergruppen, so besitzt $R \hookrightarrow A$ eine relative Ganzheitsbasis. Maurer scheint dies jedoch nicht erkannt zu haben. Außerdem beweist er den Hilfssatz nur für abelsche Erweiterungen.

Abschließend sei ein weiteres Ergebnis (Satz 1.42.) aus Kapitel 1 angeführt: Ist die Galoisgruppe G abelsch, so sind die drei Invarianten Homomorphismen und bilden das kommutative Diagramm

$$\begin{array}{ccc}
 \text{Gal}(R, G) & \xrightarrow{\text{pic}_R^G} & \text{Pic}(R [G]) \\
 \text{dis}_R^G \downarrow & \searrow \text{det}_R^G & \downarrow \text{sign}^* \\
 \text{Dis}(R) & \xrightarrow{\text{vergi\ss}} & \text{Pic}(R) \quad .
 \end{array}$$

Das rechte obere Dreieck davon verallgemeinert ein Resultat, welches Childs und Magid ([16] Proposition 3.2.) für quadratische Erweiterungen von Ringen, in denen 2 ein Nicht-Nullteiler ist, bewiesen haben.

In Kapitel 2 unterwerfen wir uns der mühsamen Pflicht, den Begriff einer verzerrten Form und den Satz über die Bijektion zwischen verzerrten Formen und Kozykelklassen in einer für unsere Zwecke günstigen Form darzustellen. Anschließend identifizieren wir mit diesen Hilfsmitteln das Invariantendiagramm als erste Čech'sche Kohomologieversion eines entsprechenden Diagrammes von Prägarben über der treuflachen Topologie.

Die Ergebnisse von Kapitel 3 verdienen wieder mehr Aufmerksamkeit. Es ist dort stets vorausgesetzt, daß 2 in R ein Nicht-Nullteiler ist. Wie schon erwähnt wurde, sind die Invarianten quadratischer Erweiterungen unter dieser Voraussetzung Glieder exakter Kohomologiefolgen.

Die exakte Kohomologiefolge zur Determinante hat das Anfangsstück ⁺)

$$0 \longrightarrow \text{Ip}(R) \longrightarrow \text{U}(R) \xrightarrow{\tau} \check{H}^0(R, W) \longrightarrow \mathcal{Q}(R) \xrightarrow{\det_R^C} \text{Pic}(R)$$

(vgl. 3.15.). Daraus gewinnt man eine Beschreibung der

⁺) Die Gruppe der quadratischen Erweiterungen von R bezeichnen wir mit $\mathcal{Q}(R)$.

Gruppe der freien quadratischen Erweiterungen als Kokern von τ . Kitamura [28] und C. Small [38] haben ähnliche Beschreibungen auf ganz andere Weise gefunden.

Die anderen beiden Invarianten lassen sich zu folgendem kommutativen Diagramm ergänzen, dessen Zeilen und Spalten Anfangsstücke exakter Kohomologiefolgen sind (vgl. 3.29. und 3.44.) :

$$\begin{array}{ccccccccccc}
 & & & & & & 0 & & 0 & & 0 \\
 & & & & & & \downarrow & & \downarrow & & \downarrow \\
 & & & 0 \longrightarrow & \text{Ip}(R) & \longrightarrow & \text{U}_2(R) & \longrightarrow & \text{U}_4(R) & & \\
 & & & & \downarrow & & \downarrow & & \downarrow & & \\
 & & & 0 \longrightarrow & \mu_2(R) & \longrightarrow & \text{U}(R) & \longrightarrow & \text{U}(R) & & \\
 & & & & \downarrow & & \downarrow & & \downarrow & & \\
 & & & 0 \longrightarrow & \text{Bi}\mu_2^4(R) & \longrightarrow & \text{U}^{(R/2R)} & \longrightarrow & \text{U}^{(R/4R)} & & \\
 & & & & \downarrow & & \downarrow & & \downarrow & & \\
 0 & \longrightarrow & \text{Ip}(R) & \longrightarrow & \text{U}_2(R) & \longrightarrow & \text{U}_4(R) & \longrightarrow & \mathcal{A}_2(R) & \longrightarrow & \mathcal{A}_4(R) \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & \mu_2(R) & \longrightarrow & \text{U}(R) & \longrightarrow & \text{U}(R) & \longrightarrow & \text{Dis}(R) & \longrightarrow & \text{Pic}(R) \longrightarrow \text{Pic}(R) \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & \text{Bi}\mu_2^4(R) & \longrightarrow & \text{U}^{(R/2R)} & \longrightarrow & \text{U}^{(R/4R)} & \longrightarrow & \check{H}^1(\text{Bi}\mu_2^4) & \longrightarrow & \text{Pic}^{(R/2R)} \longrightarrow \text{Pic}^{(R/4R)}
 \end{array}$$

$\xrightarrow{\text{pic}}$ (between $\mathcal{A}_2(R)$ and $\mathcal{A}_4(R)$)
 $\xrightarrow{\text{dis}}$ (between $\text{U}(R)$ and $\text{Dis}(R)$)

Es zeigt sich, daß wir mit diesem Resultat weit über das ursprüngliche Ziel hinausgekommen sind.

Aus der Spalte, in welcher die Diskriminante steht, ge-

winnt man die siebengliedrige exakte Folge (vgl. 3.33.)

$$0 \rightarrow \text{Ip}(R) \rightarrow \mu_2(R) \rightarrow \text{Bi} \mu_2 \pi_2^4(R) \xrightarrow{\quad} \mathcal{F}(R) \xrightarrow{\quad D \quad} U/U^2(R) \rightarrow \\ \rightarrow \frac{U(R/4R)}{U^2(R/4R)} \longrightarrow \frac{U(R/4R)}{U^2(R/4R) + \text{Bi} U \pi_4(R)} \rightarrow 0.$$

Damit hat man für Ringe R , in denen 2 ein Nicht-Nullteiler ist, eine Methode zur Hand, um die $\text{GF}(2)$ -Dimension von $\mathcal{F}(R)$ zu bestimmen. Insbesondere erhält man die Ergebnisse Kitamuras [28] als Folgerung. (Er hatte hinreichende Bedingungen dafür angegeben, daß D ein Monomorphismus ist.)

Symmetrisch dazu findet man eine exakte 7-Term-Folge, wenn man von der Zeile des Diagrammes ausgeht, welche die Picard-Invariante enthält. An die Stelle von D tritt dabei die Einschränkung der Picard-Invariante, die wir mit P bezeichnen. Ihr Kern $\mathcal{N}(R)$ besteht aus den quadratischen Erweiterungen mit Normalbasis.

$$0 \rightarrow \text{Ip}(R) \rightarrow U_2(R) \rightarrow U_4(R) \rightarrow \mathcal{F}(R) \xrightarrow{\quad P \quad} \frac{U(R/2R)}{\text{Bi} U \pi_2(R)} \rightarrow \\ \rightarrow \frac{U(R/4R)}{\text{Bi} U \pi_4(R)} \longrightarrow \frac{U(R/4R)}{U^2(R/4R) + \text{Bi} U \pi_4(R)} \rightarrow 0 \quad (\text{vgl. 3.36.}).$$

Als Folgerung ergibt sich eine Beschreibung von $\mathcal{N}(R)$, welche C. Small [39] auf andere Weise gefunden hatte.

An die Stelle von Smalls Kriterium für die Gleichheit von $\mathcal{N}(R)$ und $\mathcal{F}(R)$ setzen wir ein Maß für das Abweichen der beiden Gruppen voneinander.

Aus dem Diagramm läßt sich sogar noch eine dritte exakte Folge ableiten (vgl. 3.47.) :

$$\begin{aligned}
 0 \longrightarrow \mathcal{F}(R) \longrightarrow \mathcal{Q}(R) \xrightarrow{\det} \text{Pic}_{(2)}(R) \longrightarrow \frac{U(R/4R)}{U^2(R/4R) + B_1 U\pi_4(R)} \\
 \longrightarrow \frac{\mathcal{A}_4(R)}{\mathcal{A}_2^2(R)} \longrightarrow \frac{\text{Pic}_4(R)}{\text{Pic}_2^2(R)} \longrightarrow 0 .
 \end{aligned}$$

Wir haben damit Smalls Folge (vgl. [38]) zur Bestimmung der Modulstrukturen quadratischer Erweiterungen auf eine andere Weise gefunden und sie durch die beiden letzten Terme exakt ergänzt.

Doch kehren wir noch einmal zu den zwei wesentlichen neuen Ergebnissen zurück, um folgendes Kuriosum anzumerken: Einerseits war der Morphismus D gegeben und sein Kern gesucht, andererseits war gewissermaßen der Kern $\mathcal{N}(R)$ gegeben und der Morphismus gesucht. Die verblüffende Symmetrie wird allerdings erst nach der Lösung durch folgendes Diagramm klar

$$\begin{array}{ccccccc}
 & & & 0 & & & \\
 & & & \downarrow & & & \\
 & & & \text{Ke dis}(R) & & & \\
 & & & \downarrow & & & \\
 0 & \longrightarrow & \mathcal{N}(R) & \longrightarrow & \mathcal{F}(R) & \xrightarrow{P} & \frac{U(R/2R)}{\text{Bi } U\pi_2(R)} \\
 & & & & \downarrow D & & \\
 & & & & U/U^2(R) & & .
 \end{array}$$

Als Anwendung der Ergebnisse von Kapitel 3 bestimmen wir in Kapitel 4 die Gruppen $\mathcal{F}$ und $\mathcal{N}$ für alle Ordnungen in quadratischen Zahlkörpern (vgl. Tabellen S. 200 - 202 und S. 211).

Herr Prof. Dr. B. Pareigis hat mich bei dieser Arbeit betreut. Im Verlauf ihres Entstehens durfte ich stets mit seinem Rat und seiner freundlichen Unterstützung rechnen. Dafür möchte ich ihm an dieser Stelle herzlich danken.

Kapitel 1

MODULSTRUKTUREN VON GALOISERWEITERUNGEN EINES KOMMUTATIVEN RINGES DER SERRE-DIMENSION 1

Wie schon in der Einleitung ausgeführt wurde, verallgemeinern wir ein Konzept, welches für quadratische Erweiterungen wohlbekannt ist. Mit Hilfe der so gewonnenen "Determinante" und "Diskriminante" untersuchen wir dann die Frage: Welche R -Modulstrukturen können Galoiserverweiterungen von R haben?

§ 0 Einige Begriffe und Bezeichnungen

In der vorliegenden Arbeit sind Ringe stets assoziativ, unitär und kommutativ. In diesem Kapitel betrachten wir Galoiserverweiterungen eines "Grundringes" R mit Galoisgruppe G . Einer weit verbreiteten Gewohnheit folgend, bezeichnen wir Tensorprodukte über R einfach mit $\otimes$. Da G eine Gruppe von Automorphismen ist, schreiben wir die Verknüpfung multiplikativ - auch dann, wenn G abelsch ist. Für die zyklische Gruppe der Ordnung n schreiben wir deshalb $C_n = \{ t^0, t^1, \dots, t^{n-1} \}$. Das neutrale Element von G bezeichnen wir - je nach dem Zusammenhang - e , 1 oder auch id .

(1.1.) Definition. R sei ein kommutativer Ring, G eine endliche Gruppe der Ordnung n , und A sei eine R -Algebra, auf der G von links durch R -Algebrenautomorphismen operiert. E_A^G sei die Menge der Abbildungen von G nach A mit punktweiser A -Algebrenstruktur. $A \otimes A$ werde als A -Algebra via des ersten Faktors betrachtet, und $\theta: A \otimes A \longrightarrow E_A^G$ sei der durch $a \otimes b \longmapsto (g \mapsto ag(b))$ bestimmte A -Algebrenhomomorphismus. A heißt Galoiserweiterung von R mit Galoisgruppe G , falls eine der äquivalenten Bedingungen gilt (vgl. [12] Theorem 1.3. ; [29] Prop. 5.6.) :

- a.) A ist ein treuflacher R -Modul, und θ ist ein Isomorphismus.
- b.) Der Einsmorphimus $R \longrightarrow A$ ist injektiv, $R = A^G := \{a \in A \mid \forall g \in G : g(a) = a\}$, und es gibt $x_1, \dots, x_n, y_1, \dots, y_n \in A$ mit $\sum_{i=1}^n x_i g(y_i) = \delta_{1,g}$ für $g \in G$.
- c.) A ist ein endlich erzeugter projektiver R -Modul, $G \longrightarrow R\text{-Mod}(A, A)$ ist injektiv, und G ist ein freies A -Erzeugendensystem von $R\text{-Mod}(A, A)$ bezüglich der A -Struktur im kovarianten Argument.

Bekanntlich ist bei einer Galoiserweiterung kommutativer Ringe die Galoisgruppe nicht eindeutig bestimmt [42]. Da es im folgenden von entscheidender Bedeutung sein wird, bezüglich welcher Gruppe eine bestimmte Erweiterung galoissch ist, nennen wir eine Galoiserweiterung mit Galoisgruppe G abkürzend "G-Galoiserweiterung".

(1.2.) Bezeichnungen. Für einen kommutativen Ring R und eine endliche Gruppe G bezeichnen wir mit $\underline{R\text{-Mod}}$, $\underline{P(R)}$, $\underline{Pic(R)}$, $\underline{R\text{-Alg}}$, $\underline{Gal(R, G)}$, die Kategorien der R -Moduln, endlich erzeugten projektiven R -Moduln, invertierbaren R -Moduln, kommutativen R -Algebren, G -Galoiserweiterungen von R . Für die ersten vier davon ist es klar, welche Morphismen gemeint sind, bei den G -Galoiserweiterungen nehmen wir mit der G -Struktur verträgliche R -Algebrenhomomorphismen. $\underline{Gal(R, C_2)}$, die Kategorie der quadratischen Erweiterungen, bezeichnen wir auch mit $\underline{Q(R)}$.

$\underline{Me}$, $\underline{Grp}$, $\underline{f\text{-Grp}}$, $\underline{Ab}$, $\underline{Ri}$, sind die Kategorien der Mengen, Gruppen, endlichen Gruppen, abelschen Gruppen, kommutativen Ringe. $\underline{Pic(R)}$, $\underline{Gal(R, G)}$, $\underline{Q(R)}$ sind die Mengen der Isomorphieklassen der jeweiligen Kategorie. (Harrison zeigt, daß dies tatsächlich Mengen sind [26].) Die Isomorphieklasse eines Objektes A bezeichnen wir in all diesen Fällen mit $[A]$.

$\underline{Gal(-, -)} : \underline{Ri} \times \underline{f\text{-Grp}} \longrightarrow \underline{Me}$ ist ein Bifunktor. Für einen Ringhomomorphismus $q : R \longrightarrow S$ und einen Gruppenhomomorphismus $p : G \longrightarrow H$ wird $[A] \in \underline{Gal(R, G)}$ folgendermaßen abgebildet $\underline{Gal}(q, G)([A]) = [A \otimes_q S]$, $\underline{Gal}(R, p)([A]) = [\{ v \in \underline{Me}(H, A) \mid v(p(x)y) = xv(y), \text{ für } x \in G, y \in H \}]$. Ist p surjektiv mit Kern D , so gilt $\underline{Gal}(R, p)([A]) = [A^D]$ (vgl. [23], [35]).

Auch an den Spur-Homomorphismus sei erinnert. Für eine G -Galoiserweiterung $R \hookrightarrow A$ ist dies ein surjektiver

R-Homomorphismus $\text{tr}_R^A : A \longrightarrow R$, der durch die Vorschrift $x \longmapsto \sum_{g \in G} g(x)$ bestimmt ist ([17] Chap.3, §2).

§ 1 Determinanten von Galoiserweiterungen

C. Small [38] betrachtet für quadratische Erweiterungen die Invariante $Q(R) \ni [A] \longmapsto [\text{Ke}(\text{tr}_R^A)] \in \text{Pic}(R)$.

Die vom Spur-Homomorphismus induzierte R-direkte Zerlegung $A \simeq R \oplus \text{Ke}(\text{tr}_R^A)$ zeigt, daß die R-Modulstruktur von A durch $[\text{Ke}(\text{tr}_R^A)]$ bis auf Isomorphie bestimmt ist.

Sucht man nach einem analogen Konzept für Galoiserweiterungen mit einer beliebigen Galoisgruppe, so bietet sich zunächst folgende Möglichkeit an.

(1.3.) Eine Galoiserweiterung $R \hookrightarrow A$ mit einer Galoisgruppe G der Ordnung n ist als R-Modul endlich erzeugt projektiv und hat konstanten Rang n ([12] Lemma 4.1.). Die n-te äußere Potenz $\bigwedge_R^n(A)$ ist deshalb ein invertierbarer R-Modul ([11] Chap. 3). Der Funktor $\bigwedge_R^n : \underline{\text{Gal}}(R, G) \longrightarrow \underline{\text{Pic}}(R)$ stimmt bis auf einen Vergrößerungsfunktor mit dem Determinantenfunktor $\det$, im Sinn von Bass ([6] Chap. 9), überein:

$$\begin{array}{ccc} \underline{\text{Gal}}(R, G) & \xrightarrow{\quad \bigwedge_R^n \quad} & \underline{\text{Pic}}(R) \\ \downarrow \text{vergrößer} & \nearrow \det & \\ \underline{P}(R) & & \end{array}$$

. Für $f \in \underline{\text{Gal}}(R, G)$ (A, B)

ist $\bigwedge_R^n(f)$ die Zuordnung $\bigwedge_R^n(A) \ni x_1 \wedge \dots \wedge x_n \mapsto f(x_1) \wedge \dots \wedge f(x_n) \in \bigwedge_R^n(B)$.

Definition. Die davon induzierte Abbildung $\det_R^G : \text{Gal}(R, G) \rightarrow \text{Pic}(R)$ nennen wir — in Anlehnung an Bass — "Determinante".

Da für einen Ringhomomorphismus $q: R \rightarrow S$ die S -Moduln $\bigwedge_R^n(A) \otimes_R q^* S \simeq \bigwedge_S^n(A \otimes_R q^* S)$ isomorph sind ([6] Chap. 9), ist die Determinante funktoriell in R .

(1.4.) Der Satz von Serre weist einen Weg, um von der Determinante einer Klasse $[A]$ zur Modulstruktur der Galoiserweiterung A zu gelangen. Er besagt:

Ist R ein kommutativer Ring mit noetherschem Maximalspektrum der Dimension ≤ 1 , so läßt sich ein endlich erzeugter projektiver R -Modul A mit konstantem Rang n in eine R -direkte Summe aus $(n-1)$ Kopien von R und einem invertierbaren R -Modul P zerlegen ([6] Chap. 4, Cor. 2.7.; Chap. 9, Cor. 3.8.).

Der Isomorphismus $\bigwedge_R^n(A) \simeq \bigwedge_R^n(R^{n-1} \oplus P) \simeq \bigwedge_R^{n-1}(R^{n-1}) \otimes P \simeq R \otimes P \simeq P$ (vgl. [6] Chap. 9, S. 462) zeigt, daß über einem Ring R mit dieser Eigenschaft die Gruppenordnung und die Determinante die R -Modulstruktur einer Galoiserweiterung bis auf Isomorphie bestimmen.

Definition. Wir greifen eine Bezeichnung von Garfinkel

und Orzech auf und sagen, ein kommutativer Ring R habe Serre-Dimension ≤ 1 , wenn jeder endlich erzeugte projektive R -Modul mit konstantem Rang die direkte Summe eines freien und eines invertierbaren R -Moduls ist ([23] S. 247).

Die für uns interessante Eigenschaft dieser Ringe formulieren wir noch einmal explizit, :

Sind R ein kommutativer Ring der Serre-Dimension ≤ 1 , G eine endliche Gruppe der Ordnung n und $R \hookrightarrow A$ eine G -Galoiserweiterung, so sind $A \simeq R^{n-1} \oplus \bigwedge_R^n(A)$ isomorphe R -Moduln.

(1.5.) Beispiele. Kommutative noethersche Ringe mit Krull-Dimension ≤ 1 , insbesondere artinsche Ringe und Dedekindringe, haben Serre-Dimension ≤ 1 (vgl. Serres Satz).

Anderson konstruiert Ringe R mit einem direkt unzerlegbaren endlich erzeugten projektiven R -Modul P vom konstanten Rang ≥ 2 . Er zeigt z.B., daß $R[X, Y^2, Y(X^2+Y^2-1)] \hookrightarrow R[X, Y]$ ein solcher Ring ist ([1] Ex. 6.8.). Diese Ringe haben offensichtlich nicht die Serre-Dimension ≤ 1 .

Wenn wir im folgenden die Determinante $\det_R^G: \text{Gal}(R, G) \rightarrow \text{Pic}(R)$ betrachten, so studieren wir also — wie im Titel dieses Kapitels angekündigt — die Modulstrukturen von Galoiserweiterungen. Im Moment sind wir allerdings weit davon entfernt, ein taugliches Instrument zu haben, um Aussagen über diese Modulstrukturen zu ge-

winnen. Bisher haben wir nur eine Definition, die erst noch mit Leben zu füllen ist.

(1.6.) Proposition. $R \hookrightarrow A$ sei eine G-Galoiserweiterung, $G = \{g_1, \dots, g_n\}$ sei nummeriert, und für $x_1, \dots, x_n \in A$ bezeichne $(g_i(x_j))$ eine $(n \times n)$ -Matrix mit Zeilenindex i und Spaltenindex j .

Dann ist die Zuordnung $\gamma: \bigwedge_R^n(A) \rightarrow A$,
 $x_1 \wedge \dots \wedge x_n \mapsto \det(g_i(x_j))$ wohldefiniert, R -linear, injektiv und funktoriell in A .

Beweis. Wir zeigen: γ ist die Komposition der Morphismen

$$\begin{array}{ccccccc} \bigwedge_R^n(A) & \longrightarrow & A \otimes_R^n(A) & \xrightarrow{\sim} & \bigwedge_A^n(A \otimes_R A) & \longrightarrow & \bigwedge_A^n(E_A^G) \xrightarrow{\sim} A. \\ x \mapsto 1 \otimes x & & \text{kan} & & \bigwedge_A^n(\Theta) & & \text{kan} \end{array}$$

Die beiden kanonischen Isomorphismen bedeuten dabei "Skalarbereichserweiterung" und " $\bigwedge_A^n(A^n) \simeq A$ " ([11] Chap. 3.).

Der erste Morphismus ist injektiv, da A ein treuflacher R -Modul ist ([29] S.30). Bezeichnet $\{v_j \mid j=1, \dots, n\}$ die zu G duale Basis in E_A^G , so operieren diese Morphismen wie

$$\begin{aligned} & \text{folgt: } x_1 \wedge \dots \wedge x_n \mapsto 1 \otimes (x_1 \wedge \dots \wedge x_n) \mapsto (1 \otimes x_1) \wedge \dots \wedge (1 \otimes x_n) \\ & \mapsto \left(\sum_{j=1}^n g_j(x_1) v_j \right) \wedge \dots \wedge \left(\sum_{j=1}^n g_j(x_n) v_j \right) \\ & \mapsto \sum_{\pi \in S_n} \varepsilon(\pi) \prod_{j=1}^n g_{\pi(j)}(x_j) = \det(g_i(x_j)). \end{aligned}$$

Es bleibt noch die Natürlichkeit in A zu zeigen. Für

$f \in \text{Gal}(R, G)$ (A, B) bilden wir dazu das Quadrat

$$\begin{array}{ccc} \bigwedge_R^n(A) & \xrightarrow{\gamma} & A \\ \downarrow \bigwedge_R^n(f) & & \downarrow f \\ \bigwedge_R^n(B) & \xrightarrow{\gamma} & B. \end{array}$$

$$\begin{aligned}
 & \text{Es kommutiert, denn für } x_1 \wedge \dots \wedge x_n \in \wedge_R^n(A) \text{ ist} \\
 & \gamma \wedge_R^n(f) (x_1 \wedge \dots \wedge x_n) = \det(g_i(f(x_j))) = \det(f(g_i(x_j))) \\
 & = \sum_{\pi \in S_n} \varepsilon(\pi) \prod_{j=1}^n f(g_{\pi(j)}(x_j)) \\
 & = f\left(\sum_{\pi \in S_n} \varepsilon(\pi) \prod_{j=1}^n g_{\pi(j)}(x_j)\right) = f\gamma(x_1 \wedge \dots \wedge x_n).
 \end{aligned}$$

(1.7.) Definition. In (1.3.) haben wir vereinbart, was unter der "Determinante von $[A]$ " zu verstehen ist. $\det_R^G([A])$ ist eine Isomorphieklasse invertierbarer R -Moduln. Demgegenüber wollen wir das Bild der Einbettung $\gamma: \wedge_R^n(A) \hookrightarrow A$ die "Determinante von A " nennen und mit $\det_R^G(A)$ bezeichnen. Wie wir gerade gesehen haben, ist $\det_R^G: \text{Gal}(R, G) \rightarrow \text{Pic}(R)$ ein Funktor, welcher auf den Morphismen durch Einschränkung operiert.

In einem ersten Schritt haben wir nun $\wedge_R^n(A)$ durch den dazu isomorphen Untermodul $\det_R^G(A) \hookrightarrow A$ ersetzt. Als nächstes zeigen wir, daß $\det_R^G(A)$ mit dem Fixuntermodul $A^{\text{sign}_R^G}$ übereinstimmt. Worum es sich dabei handelt, soll im folgenden geschildert werden.

(1.8.) Bezeichnungen. Wie vorher seien R ein kommutativer Ring und G eine endliche Gruppe. Da die Einheitengruppe $U(R)$ kommutativ ist, trägt die Menge der Gruppenhomomorphismen $\text{Grp}(G, U(R))$ die Struktur einer abelschen Gruppe. Wir nennen sie Charaktergruppe und ihre Elemente Charaktere. Für eine G -Galoiserweiterung A von R und einen Charakter χ bezeichnen wir mit A^χ den Fix-

untermodul von A bezüglich $\chi : A^\chi = \{x \in A \mid \forall g \in G : g(x) = \chi(g) x\}$.

(1.9.) Proposition. (vgl. [14] 1.4.). Für eine G -Galois-erweiterung $R \hookrightarrow A$ ist die Zuordnung $\text{Grp}(G, U(R)) \ni \chi \mapsto [A^\chi] \in \text{Pic}(R)$ ein Homomorphismus abelscher Gruppen.

Beweisidee. Für einen Charakter χ ist $G \ni g \mapsto \chi(g) \in U(A)$ ein 1-Kozykel der Gruppe G mit Werten in $U(A)$, denn $\chi(gh) = \chi(g)\chi(h) = \chi(g)g\chi(h)$. Da die Gruppenstruktur bei Charakteren und bei Kozykeln punktweise definiert ist, erhält man dadurch einen Homomorphismus $\text{Grp}(G, U(R)) \longrightarrow Z^1(G, U(A))$. Verknüpft man ihn mit der Inversenbildung und dem Homomorphismus $H^1(G, U(A)) \longrightarrow \text{Pic}(R)$ aus der 7-Term-Folge von Chase, Harrison, Rosenberg ([12] Cor. 5.5.), so entsteht die beschriebene Zuordnung (vgl. [17] Chap. 4, § 2).

(1.10.) Bemerkung. Hinter der Bildung von A^χ steckt ein Galois-Abstieg (vgl. [29] II § 5). Die Abstiegsdaten sind $\bar{g} : A \ni x \mapsto \chi(g)^{-1} g(x) \in A, g \in G$.

Nun soll der Charakter sign_R^G definiert werden. Dabei bemühen wir uns um eine Exaktheit, die an dieser Stelle etwas lästig erscheint. Sie wird sich aber im folgenden als nützlich erweisen.

(1.11.) Definition. Für einen kommutativen Ring R und eine endliche Gruppe G der Ordnung n sei die "Signatur von G in R " durch folgendes Diagramm definiert

$$\begin{array}{ccc}
 G & \xrightarrow{\text{sign}_R^G} & U(R) \\
 \lambda \downarrow & & \uparrow \text{kan} \\
 S_n & \xrightarrow{\varepsilon} & \{\pm 1\}
 \end{array}$$

Dabei ist S_n die symmetrische Gruppe, und ε ordnet einer Permutation ihr Vorzeichen zu, das wir vermöge kan als Element der Einheitengruppe von R auffassen. λ schickt ein $g \in G$ auf die Linkstranslation mit g . Genauer: Bezeichnet σ die Bijektion $\{1, \dots, n\} \ni i \mapsto g_i \in G$, so ist λ durch die Vorschrift

$$\lambda(h)(i) := \sigma^{-1}(hg_i), \quad h \in G, \quad 1 \leq i \leq n \text{ bestimmt.}$$

Die Signatur ist also ein Gruppenhomomorphismus.

Damit können wir nun den entscheidenden Satz formulieren, von dem letztlich dieses ganze Kapitel lebt.

(1.12.) Satz. Für einen kommutativen Ring R , eine endliche Gruppe G und eine G -Galoiserweiterung A von R sind $\det_R^G(A) = A^{\text{sign}_R^G}$ identische Teilmengen von A .

Der Vorteil dieser neuen Beschreibung der Determinante liegt auf der Hand: für ein Element $x \in A$ ist es viel leichter, die Gültigkeit der Gleichungen

$$g(x) = \text{sign}_R^G(g) x, \quad g \in G$$

nachzuprüfen, als zu entscheiden, ob x in der Form

$$\sum_{\pi \in S_n} \varepsilon(\pi) \prod_{j=1}^n g_{\pi(j)}(x_j) \text{ darstellbar ist.}$$

Zum Beweis dieses Satzes benötigen wir noch folgende Aussage:

(1.13.) Proposition. Die Multiplikation einer G-Galoiserweiterung $R \hookrightarrow A$ induziert einen Isomorphismus

$$A \otimes_R \underline{\det}_R^G(A) \xrightarrow{\sim} A \quad \text{von } A\text{-Moduln.}$$

Beweis von (1.13.) Seien $x_1, \dots, x_n, y_1, \dots, y_n \in A$ gemäß (1.1.b.). Wie in (1.6.) bilden wir Matrizen $(g_i(x_k))$ und $(g_j(y_k))$. Die Komponente am Schnittpunkt der i-ten Zeile mit der j-ten Spalte der Produktmatrix $(g_i(x_k)) (g_j(y_k))^t$ ist

$$\sum_{k=1}^n g_i(x_k) g_j(y_k) = g_i \left(\sum_{k=1}^n x_k g_i^{-1} g_j(y_k) \right) =$$

$$g_i \left(\delta_{1, g_i^{-1} g_j} \right) = \delta_{g_i, g_j} = \delta_{i, j}.$$

Die A-lineare Abbildung $A \otimes \underline{\det}_R^G(A) \rightarrow A$ ist folglich surjektiv. Da beide A-Moduln endlich erzeugt projektiv mit konstantem Rang 1 sind, ist die Zuordnung sogar bijektiv.

Beweis von (1.12.). Zunächst weisen wir die Inklusion $\underline{\det}_R^G(A) \subseteq A^{\text{sign}_R^G}$ nach. Seien dazu $x \in \underline{\det}_R^G(A)$ und $h \in G$. Dann gibt es $x_1, \dots, x_n \in A$, so daß

$$x = \sum_{\pi \in S_n} \varepsilon(\pi) \prod_{j=1}^n g_{\pi(j)}(x_j) \quad \text{ist (vgl. 1.6. und 1.7.).}$$

$$\text{Damit gilt } h(x) = \sum_{\pi \in S_n} \varepsilon(\pi) \prod_{j=1}^n h(g_{\pi(j)}(x_j))$$

$$= \sum_{\pi \in S_n} \text{sign}_R^G(h) \varepsilon(\lambda(h)\pi) \prod_{j=1}^n g(\lambda(h)\pi)(j) (x_j)$$

(Nach 1.11. ist $hg_{\pi}(j) = g_{\lambda(h)(\pi(j))} \cdot$)

$$= \text{sign}_R^G(h) \left(\sum_{\pi \in S_n} \varepsilon(\pi) \prod_{j=1}^n g_{\pi(j)}(x_j) \right)$$

$$= \text{sign}_R^G(h) x. \text{ Also ist } x \in A^{\text{sign}_R^G}.$$

Nun zeigen wir, daß die Inklusion $q: \underline{\det}_R^G(A) \hookrightarrow A^{\text{sign}_R^G}$ auch surjektiv ist. Dazu betrachten wir das Diagramm

$$\begin{array}{ccc} A \otimes \underline{\det}_R^G(A) & \xrightarrow{A \otimes q} & A \otimes A^{\text{sign}_R^G} \\ \searrow \text{mult} & & \swarrow \text{mult} \\ & A & \end{array}$$

. Es ist kommutativ.

Die linke Seite $A \otimes \underline{\det}_R^G(A) \rightarrow A$ ist ein Isomorphismus (1.13.). Auch die rechte Seite ist ein Isomorphismus (vgl. [17] Chap. 4, § 2, S.117). (Dies folgt auch daraus, daß es sich bei der Bildung von $A^{\text{sign}_R^G}$ um einen Galois-Abstieg handelt (1.10.)). $A \otimes q$ ist also ein Isomorphismus. Da A ein treuflacher R -Modul ist (1.1.a.), ist bereits q ein Isomorphismus.

Einige naheliegende Folgerungen können wir sofort ziehen, andere müssen wir zurückstellen, bis wir über den Charakter sign_R^G besser Bescheid wissen.

(1.14.) Folgerung. $R \hookrightarrow A$ sei eine G -Galoiserweiterung. Ist $\text{sign}_R^G: G \rightarrow U(R)$ trivial, so ist $\underline{\det}_R^G(A) = R$. Im anderen Fall ist $\underline{\det}_R^G(A)$ im Kern des Spurhomomorphismus enthalten.

Beweis. Sei $\text{sign}_R^G = 1$. Dann ist $\underline{\det}_R^G(A) = \{x \in A \mid \forall g \in G : g(x) = \text{sign}_R^G(g)x\} = A^G = R$.

Seien nun $\text{sign}_R^G \neq 1$ und $h \in G$ ein Element mit negativer Signatur. Dann gilt für alle $x \in \underline{\det}_R^G(A)$

$$\begin{aligned} \text{tr}_R^A(x) &= \sum_{g \in G} g(x) = \sum_{g \in \text{Ke}(\text{sign}_R^G)} (g(x) + hg(x)) \\ &= \sum_{g \in \text{Ke}(\text{sign}_R^G)} (\text{sign}_R^G(g) + \text{sign}_R^G(hg)) x = 0. \end{aligned}$$

(1.15.) Folgerung. Für eine quadratische Erweiterung $R \hookrightarrow A$ sind $\underline{\det}_R^{C^2}(A) = \text{Ke}(\text{tr}_R^A)$ identische Teilmengen von A . Unsere Determinante $\det_R^G: \text{Gal}(R, G) \rightarrow \text{Pic}(R)$ (vgl. 1.3.) stimmt also im quadratischen Fall mit der von Revoy und C. Small betrachteten Invariante überein [36, 38].

Beweis. Die Galoisgruppe ist in diesem Fall $C_2 = \{1, t\}$. Für $x \in \text{Ke}(\text{tr}_R^A)$ ist $0 = \text{tr}_R^A(x) = x + t(x)$, also ist $t(x) = -x = \text{sign}_R^{C^2}(t)x$. Deshalb gilt in diesem Fall auch die Inklusion $\text{Ke}(\text{tr}_R^A) \subseteq \underline{\det}_R^{C^2}(A)$.

(1.16.) Folgerung. Seien R ein kommutativer Ring der Serre-Dimension 1 und G eine endliche Gruppe. Ist $\text{sign}_R^G: G \rightarrow U(R)$ der triviale Charakter, so sind alle G -Galoiserweiterungen als R -Moduln frei.

Beweis. Die Ordnung von G sei n . Für eine G -Galoiserweiterung $R \hookrightarrow A$ sind dann folgende R -Moduln isomorph $A \simeq R^{n-1} \oplus \bigwedge_R^n(A) \simeq R^n$ (vgl. 1.4. und 1.14.).

§ 2 Der Charakter "Signatur"

Durch das zuletzt erzielte Ergebnis ist unsere Beschäftigung mit dem Homomorphismus sign_R^G hinreichend motiviert. Dabei wird uns die Exaktheit der Definition (1.11.) zugute kommen.

(1.17. Proposition. Für $g \in G$ seien $\text{ord}(g)$ und $\text{ind}(g)$ Ordnung und Index der von g erzeugten Untergruppe. Dann ist $\varepsilon \lambda(g) = (-1)^{\text{ind}(g) \cdot (\text{ord}(g)-1)}$.

Beweis. Sei $g \in G$. $\lambda(g)$ läßt sich in ein Produkt von paarweise elementfremden Zykeln zerlegen. Diese zyklischen Faktoren haben die Gestalt $(i, \lambda(g)(i), \lambda(g)^2(i), \dots) = (i, \sigma^{-1}(g g_i), \sigma^{-1}(g^2 g_i), \dots)$, wobei i ein Repräsentantensystem der Zykeln durchläuft. Vermöge der Bijektion σ entspricht einem solchen Faktor ein geordnetes Tupel von Gruppenelementen $(g_i, g g_i, g^2 g_i, \dots)$.

Die Länge dieses Zyklus ist die kleinste natürliche Zahl l , für welche $i = \lambda(g)^l(i)$ ist. $i = \lambda(g)^l(i) \iff \sigma(i) = g^l \sigma(i) \iff e = g^l$ (=neutrales Element von G).

Also ist l die Ordnung von g , und die Zykeln entsprechen den Nebenklassen der von g erzeugten Untergruppe. Die Behauptung folgt nun daraus, daß $\varepsilon : S_n \longrightarrow \{\pm 1\}$ ein Gruppenhomomorphismus ist und das Vorzeichen eines Zyklus der Länge l gleich $(-1)^{l-1}$ ist.

(1.18.) Korollar. Mit den Bezeichnungen von (1.17.) gilt:

$$\text{sign}_R^G(g) \neq +1 \iff \left\{ \begin{array}{ll} \text{i.)} & \text{ord}(g) \equiv 0(2) \\ \text{ii.)} & \text{ind}(g) \equiv 1(2) \\ \text{iii.)} & 2 \neq 0 \text{ in } R \end{array} \right\}.$$

Beweis. Klar.

Die Beschreibung der Gruppen G mit nicht-trivialer Signatur ist eine Übungsaufgabe von Bourbaki ([11] Chap. 1, S. 139, Exerc. 29). Wir wollen auf ihren Beweis dennoch nicht verzichten, da sie im folgenden eine wichtige Rolle spielen wird.

(1.19.) Proposition. a.) Ist $2 \neq 0$, so ist sign_R^G genau dann nicht-trivial, wenn G eine zyklische 2-Sylowuntergruppe $H \neq 0$ besitzt.

b.) Ist G eine endliche Gruppe und $0 \neq H$ eine zyklische 2-Sylowuntergruppe von G , dann gibt es genau einen Normalteiler D von G , so daß G semidirektes Produkt von D und H ist. Der Normalteiler D besteht aus allen Elementen ungerader Ordnung.

Beweis. a.) Mit Korollar (1.18.) sieht man: Ist $\epsilon \in \lambda$ surjektiv, so hat G eine zyklische Untergruppe mit gerader Ordnung und ungeradem Index. In ihr finden wir dann eine zyklische 2-Sylowuntergruppe $H \neq 0$ von G . Andererseits gilt für ein erzeugendes Element t einer zyklischen 2-Sylowuntergruppe $H \neq 0$ von G : $\text{sign}_R^G(t) = -1$.

Bemerkung. Wenn wir sagen, daß G semidirektes Produkt eines Normalteilers D und einer Untergruppe H ist, so setzen wir stillschweigend voraus, daß H auf D durch innere Automorphismen operiert. Mit

Hilfe von ([11] Chap. 1, § 6, Prop. 4) überlegt man sich leicht, daß G genau dann semidirektes Produkt von D und H ist, wenn es einen surjektiven Gruppenhomomorphismus $p : G \longrightarrow H$ mit Kern D gibt, der die Elemente von H fix läßt.

Beweis von (1.19.b). Wir schreiben die Gruppenordnung in der Form $n = 2^a m$, $a \geq 1$, $2 \nmid m$ und führen einen Induktionsbeweis nach a . Für $a = 1$ ist $\varepsilon\lambda : G \longrightarrow \{\pm 1\} \cong H$ der einzige surjektive Homomorphismus $G \longrightarrow H$, welcher die Elemente von H fix läßt. Sein Kern besteht aus den Elementen ungerader Ordnung. Nun schließen wir von a auf $a+1$: G habe die Ordnung $2^{a+1}m$, und H sei eine 2-Sylowuntergruppe von G . Der Homomorphismus $\varepsilon\lambda$ ist surjektiv, $\overline{G} := \text{Ke}(\varepsilon\lambda)$ hat also die Ordnung $2^a m$. Ist t ein erzeugendes Element von H , so ist $\varepsilon\lambda(t) = -1$, und die Ordnung von $\overline{H} := \overline{G} \cap H = \langle t^2 \rangle$ ist 2^a . Sei $\overline{G} = D \rtimes \overline{H}$ die Zerlegung von $\overline{G}$ gemäß der Induktionsannahme. Da H nur Elemente gerader Ordnung enthält, ist $D \cap H = \{e\}$. Wenn wir noch zeigen, daß $D \cdot H = G$ und D ein Normalteiler von G ist, dann gilt $G = D \rtimes H$. $G = D \rtimes H$: Sei $g \in G$. Ist $g \in \overline{G}$, so gibt es $d \in D$, $i \in \mathbb{Z}$ mit $g = d t^{2i}$. Falls $g \notin \overline{G}$, dann ist $gt^{-1} \in \overline{G}$, und es existieren $d \in D$, $i \in \mathbb{Z}$ mit $g = dt^{2i+1}$. $D \triangleleft G$: Seien $d \in D$, $g \in G$. Ist $g \in \overline{G}$, so ist $gdg^{-1} \in D$, denn $D \triangleleft \overline{G}$. Da $\overline{G}$ in G normal ist, liegt tdt^{-1} in $\overline{G}$. Der Automorphismus $t(\)t^{-1}$ läßt die Ordnung des

Elementes d unverändert. Deshalb ist tdt^{-1} sogar in D . Falls nun $g \notin \bar{G}$, so ist $gt^{-1} \in \bar{G}$ und $gdg^{-1} = (gt^{-1})tdt^{-1}(gt^{-1})^{-1} \in D$.

Die Elemente von G haben also eindeutige Darstellungen der Form dt^i mit $d \in D$, $0 \leq i \leq 2^a - 1$. Sie werden folgendermaßen verknüpft $(dt^i)(d't^j) = dt^i d' t^{-i} t^{i+j}$. Damit sieht man $D = \{g \in G \mid \text{ord}(g) \equiv 1(2)\}$.

Sei nun D' ein weiterer Normalteiler von G , so daß $G = D' \not\equiv H$ ist. Sei $p' : G \rightarrow H$ ein surjektiver Homomorphismus mit Kern D' , welcher die Elemente von H fix läßt. Dann gilt für $d \in D$, $i \in \mathbb{Z} : p'(dt^i) = p'(d)t^i = t^i$, denn $\text{ord}(p'(d)) \equiv 1(2)$. Dies zeigt $D' = D$.

(1.20.) Beispiele. a.) Die Umkehrung von (1.19.b) gilt nicht. Auch wenn zu einer 2-Sylowuntergruppe $H \neq 0$ genau ein Normalteiler D die Gleichung $G = D \not\equiv H$ erfüllt, so ist H im allgemeinen nicht zyklisch. In $C_3 \times C_2 \times C_2$ ist $0 \times C_2 \times C_2$ eine nicht-zyklische 2-Sylowuntergruppe, und $C_3 \times 0 \times 0$ ist die einzige Untergruppe der Ordnung 3.

b.) In der Situation von (1.19.b) ist D eindeutig und unabhängig von der 2-Sylowuntergruppe H . Doch es gibt im allgemeinen mehrere 2-Sylowuntergruppen. In der symmetrischen Gruppe S_3 ist der Normalteiler der Elemente ungerader Ordnung die alternierende Gruppe A_3 . Aber S_3 besitzt drei zyklische 2-Sylowuntergruppen.

§ 3 Diskriminanten von Galoiserweiterungen

Für die Untersuchung der Modulstrukturen von Galoiserweiterungen ist es günstig, auch die zweite der angekündigten beiden Invarianten zur Verfügung zu haben. Aus diesem Grund schieben wir noch den vorliegenden Abschnitt ein, bevor wir uns der eigentlichen Fragestellung von Kapitel 1 zuwenden.

(1.21.) Definition. Wir schließen uns Bass [7] an und bezeichnen für einen kommutativen Ring R die Kategorie der R -Diskriminantenmoduln mit $\text{Dis}(R)$. Ihre Objekte (P, α) sind invertierbare R -Moduln P zusammen mit einer nichtausgearteten Bilinearform α . Morphismen $f : (P, \alpha) \longrightarrow (P', \alpha')$ sind mit den Bilinearstrukturen verträgliche R -Modulhomomorphismen. Durch Lokalisieren zeigt man das nützliche Kriterium: eine Bilinearform α auf einem invertierbaren R -Modul P ist genau dann nicht-ausgeartet, wenn α einen R -Modulisomorphismus $P \otimes_R P \xrightarrow{\sim} R$ induziert (vgl. [7] S. 164). Wie in (1.2.) schreiben wir $\text{Dis}(R)$ für die Menge der Isomorphieklassen von $\text{Dis}(R)$.

Micali, Villamayor [33] und Revoy [36] betrachteten für quadratische Erweiterungen eine Invariante $\mathcal{Q}(R) \longrightarrow \text{Dis}(R)$. Die entscheidende Beobachtung war dabei, daß für eine quadratische Erweiterung $R \hookrightarrow A$ die Multiplikation von A auf $\text{Ke}(\text{tr}_R^A)$ eine nicht-ausgeartete Bilinearform in-

duziert. Auf dieselbe Weise wird nun unsere "Diskriminante"
 $\text{dis}_R^G : \text{Gal}(R, G) \longrightarrow \text{Dis}(R)$ zustande kommen.

(1.22.) Proposition. Seien R ein kommutativer Ring, G eine endliche Gruppe der Ordnung n und A eine G -Galois-
 erweiterung von R . Auf der n -ten äußeren Potenz $\bigwedge_R^n(A)$
 ist durch folgende Zuordnung eine nicht-ausgeartete Bilinear-
 form gegeben

$$\begin{aligned} \mu_A : \bigwedge_R^n(A) \times \bigwedge_R^n(A) &\longrightarrow R \\ (x_1 \wedge \dots \wedge x_n, y_1 \wedge \dots \wedge y_n) &\longmapsto \det(\text{tr}_R^A(x_i y_j)). \end{aligned}$$

Dadurch ist ein Funktor $\underline{\text{Gal}}(R, G) \longrightarrow \underline{\text{Dis}}(R)$ bestimmt,
 der auf den Objekten durch $A \longmapsto (\bigwedge_R^n(A), \mu_A)$ und auf
 den Morphismen durch $f \longmapsto \bigwedge_R^n(f)$ operiert. Die in-
 duzierte Abbildung $\text{Gal}(R, G) \longrightarrow \text{Dis}(R)$ ist funktoriell
 in R .

Beweis. Eine G -Galoiserweiterung $R \hookrightarrow A$ ist separabel
 und als R -Modul treuprojektiv vom konstanten Rang n
 (1.1.). Deshalb ist die Bilinearform $\phi_A : A \times A \ni (x, y) \longmapsto$
 $\text{tr}_R^A(xy) \in R$ nicht-ausgeartet (vgl. [29] Chap. 3, Théorème
 4.7.). Für $r \geq 1$ trägt $\bigwedge_R^r(A)$ eine nicht-ausgeartete
 Bilinearform $\bigwedge_R^r(\phi_A) : \bigwedge_R^r(A) \times \bigwedge_R^r(A) \longrightarrow R$
 $(x_1 \wedge \dots \wedge x_r, y_1 \wedge \dots \wedge y_r) \longmapsto \det(\text{tr}_R^A(x_i y_j))$
 (vgl. [9] S. 30, 31). Insbesondere ist also
 $(\bigwedge_R^n(A), \bigwedge_R^n(\phi_A))$ ein Diskriminantenmodul.
 Sei nun $f \in \underline{\text{Gal}}(R, G)(A, B)$. $\bigwedge_R^n(f)$ ist mit den Bilinear-
 strukturen auf $(\bigwedge_R^n(A), \mu_A)$ und $(\bigwedge_R^n(B), \mu_B)$ verträglich,
 denn für $x_1 \wedge \dots \wedge x_n, y_1 \wedge \dots \wedge y_n \in \bigwedge_R^n(A)$ gilt

$$\begin{aligned} \mu_B(\wedge_R^n(f)(x_1 \wedge \dots \wedge x_n), \wedge_R^n(f)(y_1 \wedge \dots \wedge y_n)) &= \\ \det(\text{tr}_R^B(f(x_i) f(y_j))) &= \det\left(\sum_{g \in G} g(f(x_i x_j))\right) = \\ \det\left(f\left(\sum_{g \in G} g(x_i y_j)\right)\right) &= \det(\text{tr}_R^A(x_i y_j)). \end{aligned}$$

Damit ist nun klar, daß die beschriebenen Zuordnungen einen Funktor bilden. Es bleibt noch zu zeigen, daß für einen Ringhomomorphismus $R \rightarrow S$ der Isomorphismus $\text{kan}: \wedge_R^n(A) \otimes S \xrightarrow{\sim} \wedge_S^n(A \otimes S)$ mit den Bilinearstrukturen verträglich ist (vgl. 1.3.). Dazu ist zu zeigen, daß folgendes Diagramm kommutiert

$$\begin{array}{ccc} & \text{kan} \otimes \text{kan} & \\ (\wedge_R^n(A) \otimes_R S) \otimes_S (\wedge_R^n(A) \otimes_R S) & \xrightarrow{\sim} & \wedge_S^n(A \otimes S) \otimes_S \wedge_S^n(A \otimes S) \\ \text{kan} \downarrow \wr & & \downarrow \mu_{A \otimes S} \\ \wedge_R^n(A) \otimes_R \wedge_R^n(A) \otimes_R S & \xrightarrow{\mu_{A \otimes S}} & R \otimes_R S \xrightarrow{\sim} S \end{array}$$

Seien $s, s' \in S$ und $x_1 \wedge \dots \wedge x_n, y_1 \wedge \dots \wedge y_n \in \wedge_R^n(A)$.

$$\begin{aligned} \mu_{A \otimes S}(\text{kan} \otimes \text{kan})((x_1 \wedge \dots \wedge x_n \otimes s) \otimes (y_1 \wedge \dots \wedge y_n \otimes s')) &= \\ \mu_{A \otimes S}((x_1 \otimes s) \wedge \dots \wedge (x_n \otimes 1)) \otimes ((y_1 \otimes s') \wedge \dots \wedge (y_n \otimes 1)) & \end{aligned}$$

$$\begin{aligned} &= \begin{vmatrix} \text{tr}_R^A(x_1 y_1) \otimes s s' & \text{tr}_R^A(x_1 y_2) \otimes s & \dots & \text{tr}_R^A(x_1 y_n) \otimes s \\ \text{tr}_R^A(x_2 y_1) \otimes s' & \text{tr}_R^A(x_2 y_2) \otimes 1 & \dots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ \text{tr}_R^A(x_n y_1) \otimes s' & \text{tr}_R^A(x_n y_2) \otimes 1 & \dots & \text{tr}_R^A(x_n y_n) \otimes 1 \end{vmatrix} \\ &= \det(\text{tr}_R^A(x_i y_j)) \otimes s s' \\ &= (\mu_{A \otimes S} \text{kan})((x_1 \wedge \dots \wedge x_n \otimes s) \otimes (y_1 \wedge \dots \wedge y_n \otimes s')). \end{aligned}$$

(1.23.). Satz. Es seien R ein kommutativer Ring, G eine endliche Gruppe der Ordnung n und $R \hookrightarrow A$ eine G -Galoiserweiterung.

Die Multiplikation von A induziert eine nicht-ausgeartete Bilinearform $A^{\text{sign}_R^G} \times A^{\text{sign}_R^G} \xrightarrow{\text{mult}} R$. Bezeichnet μ_A die Bilinearform aus (1.22.), so ist die Zuordnung $\bigwedge_R^n(A) \ni x_1 \wedge \dots \wedge x_n \mapsto \det(g_i(x_j)) \in A^{\text{sign}_R^G}$ ein Isomorphismus $\gamma: (\bigwedge_R^n(A), \mu_A) \longrightarrow (A^{\text{sign}_R^G}, \text{mult})$ von Diskriminantenmoduln (vgl. 1.6., 1.12.).

(1.24.) Bezeichnungen. $(A^{\text{sign}_R^G}, \text{mult})$ nennen wir Diskriminante von A . Der Funktor $\text{dis}_R^G: \text{Gal}(R, G) \longrightarrow \text{Dis}(R)$ ordnet einer G -Galoiserweiterung ihre Diskriminante zu und operiert auf den Morphismen durch Einschränkung. Den zugehörigen natürlichen Morphismus $\text{Gal}(R, G) \longrightarrow \text{Dis}(R)$ bezeichnen wir mit dis_R^G .

Bemerkung. Im Beweis von (1.22.) haben wir den Diskriminantenmodul einer Galoiserweiterung als $(\bigwedge_R^n(A), \bigwedge_R^n(\phi_A))$ konstruiert. Die Bilinearform ϕ_A wird "Spur-Form" genannt (vgl. [30]). Unsere Invariante $\text{dis}_R^G([A])$ stimmt daher mit der "Diskriminante von $(A, \text{Spur-Form})$ ", im Sinn von Bass [7], überein.

Beweis von (1.23.). (1.6.) und (1.12.) zeigen, daß γ ein Isomorphismus von R -Moduln ist. Sind $x, y \in \det_R^G(A)$, so gilt für alle $g \in G: g(xy) = g(x) \cdot g(y) = \text{sign}_R^G(g)^2 xy = xy$. $\text{mult}: \det_R^G(A) \times \det_R^G(A) \longrightarrow A^G = R$ ist deshalb eine Bilinearform. Der Satz ist bewiesen, wenn folgendes Dreieck kommutiert

$$\begin{array}{ccc}
 \wedge_R^n(A) \otimes \wedge_R^n(A) & \xrightarrow[\sim]{\gamma \otimes \gamma} & \underline{\det}_R^G(A) \otimes \underline{\det}_R^G(A) \\
 \searrow \mu_A & & \swarrow \text{mult} \\
 & R & .
 \end{array}$$

Zum Nachweis der Kommutativität nehmen wir

$x_1 \wedge \dots \wedge x_n, y_1 \wedge \dots \wedge y_n \in \wedge_R^n(A)$. Dann gilt

$$\begin{aligned}
 & \gamma(x_1 \wedge \dots \wedge x_n) \cdot \gamma(y_1 \wedge \dots \wedge y_n) = \det(g_k(x_i)) \det(g_k(y_j)) \\
 & = \det \left((g_k(x_i))^t (g_k(y_j)) \right) = \det \left(\sum_{k=1}^n g_k(x_i) g_k(y_j) \right) = \\
 & \det(\text{tr}_R^A(x_i y_j)) = \mu_A(x_1 \wedge \dots \wedge x_n \otimes y_1 \wedge \dots \wedge y_n).
 \end{aligned}$$

(1.25.) Folgerungen.

- a.) Die Determinanten von Galoiserweiterungen haben in $\text{Pic}(R)$ eine Ordnung ≤ 2 .
- b.) Ist $\text{sign}_R^G = 1$, so sind die Diskriminanten aller G -Galoiserweiterungen zum trivialen Diskriminantenmodul $(R, 1)$ isomorph.
- c.) Für quadratische Erweiterungen stimmt $\text{dis}_R^{C_2}: \mathcal{Q}(R) \rightarrow \text{Dis}(R)$ mit der von Micali, Villamayor und Revoy betrachteten Invariante $[A] \longrightarrow [\text{Ke}(\text{tr}_R^A, \text{mult})]$ überein (vgl. [32] 3.2.; [36]).

Beweis. a.) folgt direkt aus (1.23.). Für b.) bzw. c.) zieht man noch (1.14.) bzw. (1.15.) heran.

§ 4 Modulstrukturen von Galoisweiterungen

Nun wollen wir endlich zeigen, daß unsere beiden Invarianten nicht nur "gute Eigenschaften" haben, sondern auch zu etwas zu gebrauchen sind. Deshalb stellen wir gleich zu Beginn das Hauptergebnis dieses Abschnitts vor.

(1.26.) Theorem. Für einen kommutativen Ring R der Serre-Dimension 1 und eine endliche Gruppe G der Ordnung n gilt:

- a.) Ist n ungerade, so sind alle G -Galoisweiterungen von R als R -Moduln frei.
- b.) Ist n gerade, und besitzt G nicht-zyklische 2-Sylowuntergruppen, so sind alle G -Galoisweiterungen von R als R -Moduln frei.
- c.) Ist $2 = 0$ in R , so sind alle Galoisweiterungen von R als R -Moduln frei.
- d.) Ist n gerade, und besitzt G eine zyklische 2-Sylowuntergruppe H , so treten bei G -Galoisweiterungen von R bis auf freie direkte Summanden dieselben R -Modulstrukturen auf wie bei H -Galoisweiterungen von R .

Beweis. Mit (1.18.) und (1.19.) sieht man, daß in jedem der drei Fälle a, b, c die Signatur $\text{sign}_R^G = 1$ ist. Daraus ergeben sich die Behauptungen nach (1.16.). Für den Beweis von Teil d ist noch einiges zu tun. Wir werden ihn schließ-

lich in (1.35.) erbracht haben.

(1.27.) Folgerung. Sei $K \hookrightarrow L$ eine unverzweigte Galoiserweiterung algebraischer Zahlkörper mit Galoisgruppe G . Die Erweiterung $R \hookrightarrow A$ der zugehörigen Ringe der ganzen algebraischen Zahlen besitzt eine relative Ganzheitsbasis, falls G eine der beiden folgenden Bedingungen erfüllt:

a.) Die Ordnung von G ist ungerade.

b.) G besitzt nicht-zyklische 2-Sylowuntergruppen.

Beweis von (1.27.). R ist ein Dedekindring, hat also Serre-Dimension 1 (1.5.), und wegen der Unverzweigt-heit ist $R \hookrightarrow A$ eine G -Galoiserweiterung ([12] 1.5.d). Deshalb ist das Theorem anwendbar.

(1.28.) Bemerkung. Die Aussage (1.27. a) wurde bereits von Fröhlich ([19] Theorem 4.3.) mit anderen Methoden bewiesen. Mit Hilfe eines kürzlich publizierten Resultats von Maurer [30] könnte man mit denselben Methoden auch (1.27. b) zeigen (vgl. Einleitung).

Wenn wir uns nun dem Beweis von (1.26.d) zuwenden, so können wir den trivialen Fall $2 = 0$ übergehen und befinden uns dann in der Situation : $2 \neq 0$, $n \equiv 0(2)$, und G besitzt eine zyklische 2-Sylowuntergruppe $H \neq 0$. Nach (1.19.) ist dies dazu äquivalent, daß die Signatur sign_R^G nicht-trivial ist.

(1.29.). Wir wollen deshalb nun die Determinante im Fall einer nicht-trivialen Signatur genauer betrachten. Dazu vereinbaren wir folgende Bezeichnungen (vgl. 1.19.) :

R sei ein kommutativer Ring mit $2 \neq 0$, G sei eine endliche Gruppe der Ordnung $n = 2^a m$, $a \geq 1$, $2 \nmid m$; und $H \hookrightarrow G$ sei eine zyklische 2-Sylowuntergruppe mit erzeugendem Element t ; $p : G \rightarrow H$ sei ein surjektiver Gruppenhomomorphismus, welcher die Elemente von H fix läßt. $D := \text{Ke}(p)$ besteht aus den Elementen ungerader Ordnung (1.19.).

Für $1 \leq j \leq a$ definieren wir Homomorphismen

$$p_j : G \xrightarrow[p]{\quad} H \xrightarrow[t \mapsto t]{\sim} C_{2^a} \xrightarrow[\text{kan}]{\quad} C_{2^j}. \text{ Die}$$

p_j sind surjektiv, und ihre Kerne $G_j := \text{Ke}(p_j)$ bilden eine absteigende Kette von Normalteilern von G

$$D = G_a \hookrightarrow G_{a-1} \hookrightarrow \dots \hookrightarrow G_2 \hookrightarrow G_1 \hookrightarrow G.$$

(1.30.) Satz. R und G seien wie in (1.29.). Für eine G -Galoiserweiterung $R \hookrightarrow A$ bilden die Fixringe $A_j := A^{G_j}$, $1 \leq j \leq a$ eine aufsteigende Kette von Untergruppen von A

$$R \subseteq A_1 \subseteq A_2 \subseteq \dots \subseteq A_{a-1} \subseteq A_a \subseteq A.$$

Darüber hinaus gilt: Für alle $1 \leq j \leq a$ ist A_j eine C_{2^j} -Galoiserweiterung von R , und ihre Determinante $\det_R^{C_{2^j}}(A_j)$ stimmt als Teilmenge von A mit $\det_R^G(A)$ überein.

Beweis. Die $G_j \hookrightarrow G$ sind Normalteiler mit Faktorgruppe C_{2^j} . Nach dem Fundamentalsatz der Galoistheorie ([12] Theorem 2.2.) ist $R \hookrightarrow A_j$ eine C_{2^j} -Galoiserweiterung.

Um zu zeigen, daß für $1 \leq j \leq a$ $\det_R^{C_{2^j}}(A_j) = \det_R^{C_{2^a}}(A_a)$ ist, überlegen wir: Im semidirekten Produkt $G = D \rtimes H$ sind die Elemente von der Form $d \cdot t^i$, $0 \leq i \leq 2^a - 1$, $d \in D$. Es ist $p(dt^i) = t^i$, und der Exponent von $p_j(dt^i)$ ist

der Rest der Division von i durch 2^j . Deshalb wird G_j von D und t^{2^j} erzeugt, und $A_j = \{x \in A^D \mid t^{2^j}(x) = x\}$.

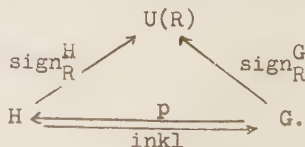
Die Galoisgruppe G/G_j zur Erweiterung $R \hookrightarrow A_j$ besitzt das Repräsentantensystem $\{t^i \mid 0 \leq i \leq 2^j - 1\}$ in G . Für

$1 \leq j \leq a$ gilt also $\det_R^{C_{2^j}}(A_j) =$

$$\{x \in A^D \mid t^{2^j}(x) = x \text{ und } t(x) = -x\} = \{x \in A_a \mid t(x) = -x\} = A_a^{\text{sign}_R^{C_{2^a}}}.$$

Zu zeigen bleibt noch, daß $\det_R^{C_{2^a}}(A_a) = \det_R^G(A)$ ist. Doch zuvor schieben wir eine Zwischenüberlegung ein.

(1.31.) Hilfssatz. Mit der Bezeichnung von (1.29.) kommutiert folgendes Dreieck für beide Grundseiten



Beweis des Hilfssatzes. Sei $dt^i \in G$. Dann ist

$$\text{sign}_R^G(dt^i) =$$

$$\text{sign}_R^G(d) \cdot \text{sign}_R^G(t^i) = \left\{ \begin{array}{l} +1, \text{ falls } i \equiv 0(2) \\ -1, \text{ falls } i \equiv 1(2) \end{array} \right\} =$$

$$= \text{sign}_R^H(t^i) = \text{sign}_R^H(dt^i). \text{ Analog sieht man}$$

$$\text{sign}_R^G \text{ inkl}(t^i) = \text{sign}_R^H(t^i).$$

Beweis des Satzes, 2. Teil. Die Galoisgruppe von

$$A_a = A^D \text{ ist } G/D \cong H.$$

$$A_a^{\text{sign}_R^H} \subseteq A^{\text{sign}_R^G} : \text{ Für } x \in A_a^{\text{sign}_R^H} \text{ und } dt^i \in G \text{ gilt}$$

$$dt^i(x) = t^i(x) = \text{sign}_R^H(t^i) \cdot x = \text{sign}_R^G(t^i) \cdot x =$$

$$= \text{sign}_R^G(d) \cdot \text{sign}_R^G(t^i) \cdot x = \text{sign}_R^G(dt^i) \cdot x. \text{ Also ist}$$

$$x \in A^{\text{sign}_R^G}.$$

$$A_a^{\text{sign}_R^H} \supseteq A^{\text{sign}_R^G} : \text{ Für } x \in A^{\text{sign}_R^G} \text{ und } t^i \in H \text{ ist}$$

$$t^i(x) = \text{sign}_R^G(t^i) \cdot x = \text{sign}_R^H(t^i) \cdot x. \text{ Also ist}$$

$$x \in A_a^{\text{sign}_R^H}.$$

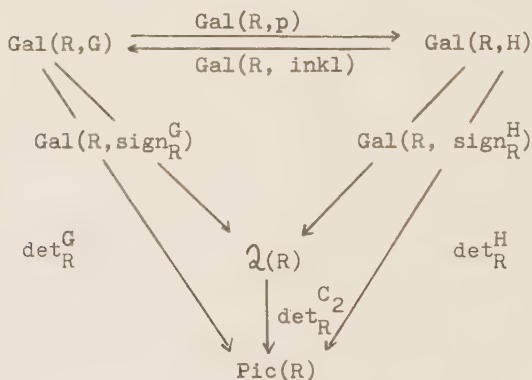
(1.32.) Beispiel. Für eine Untergruppe H einer endlichen Gruppe G ist das Dreieck von (1.31.) im allgemeinen nicht kommutativ. Ist $G = C_{12}$ und $H = \langle t^2 \rangle$, so ist $\text{sign}_R^H(t^2) = -1$, während $\text{sign}_R^G(t^2) = 1$ ist.

(1.33.) Bemerkung. Unter den Voraussetzungen von Satz (1.30.) stimmen auch die Diskriminanten überein:

$$\underline{\text{dis}}_R^G(A) = \underline{\text{dis}}_R^H(A) = \dots = \underline{\text{dis}}_R^{C_2}(A_1) .$$

Beweis. Dies folgt aus (1.23.) und (1.30.).

(1.34.) Satz. Unter den Voraussetzungen von (1.29.) kommutiert folgendes Diagramm von Mengen und Abbildungen



(1.35.) Folgerung. Unter den Voraussetzungen von (1.29.) gilt insbesondere $\text{Bi}(\det_R^G) = \text{Bi}(\det_R^H)$, womit nun auch (1.26. d) bewiesen ist.

Beweis von (1.34.) und (1.35.). Das obere Dreieck kommutiert mit beiden horizontalen Pfeilen, denn es geht durch den Funktor $\text{Gal}(R, -)$ aus (1.31.) hervor. Für das linke Dreieck folgt die Kommutativität aus der Überlegung:

$\text{Ke}(\text{sign}_R^G) = \text{Ke}(p_1) = G_1$. Also ist

$$\det_R^{C_2} \text{Gal}(R, \text{sign}_R^G)[A] = \det_R^{C_2} [A^{G_1}] = \det_R^{C_2} [A_1] = \det_R^G [A]$$

(vgl. 1.2., 1.30.). Ersetzt man in dieser Überlegung G durch H , so folgt die Kommutativität des rechten Dreiecks. Daher kommutiert auch das große Dreieck mit beiden horizontalen Pfeilen. Dies zeigt $\text{Bi}(\det_R^G) = \text{Bi}(\det_R^H)$.

(1.36.) Korollar. Aus dem Beweis von Satz (1.34.) erkennt man, daß auch das analoge Diagramm für die Diskriminanten kommutiert.

Zum Abschluß von § 4 wollen wir zwei Aussagen angeben, die zwar am Rande unseres Gebietes liegen, aber dennoch erwähnenswert sind.

(1.37.) Proposition. R sei ein kommutativer Ring, G eine endliche Gruppe und $R \hookrightarrow A$ eine G -Galoiserweiterung. Der Untermodul $\det_R^G(A) \hookrightarrow A$ ist ein R -direkter Summand.

Beweis. Ist $\text{sign}_R^G = 1$, so ist $\det_R^G(A) = A^G = R \cdot 1$ (1.14.); und $R \cdot 1$ ist in der endlich erzeugten projektiven separablen Erweiterung A ein direkter Summand ([17] Chap.3, Cor. 2.3.). Sei nun $\text{sign}_R^G \neq 1$. Wir wählen die Bezeichnungen von (1.29.). $R \hookrightarrow A_1$ ist eine quadratische Erweiterung und $A_1 \hookrightarrow A$ ist eine G_1 -Galoiserweiterung. Es gibt ein $a \in A$ mit $\text{tr}_{A_1}^A(a) = 1$, und $\mathcal{W}: A \ni x \mapsto \text{tr}_{A_1}^A(ax) \in A_1$ ist eine A_1 -lineare Retraktion zur Einbettung $A_1 \hookrightarrow A$

([17] Chap. 3). A ist also eine innere A_1 -direkte Summe $A = A_1 \oplus \text{Ke}(\pi)$. Dieselben Überlegungen zeigen, daß A_1 eine innere R -direkte Zerlegung

$A_1 = \text{Ke}(\text{tr}_R^{A_1}) \oplus R \cdot b$ besitzt, wobei b ein Element von A_1 mit $\text{tr}_R^{A_1}(b) = 1$ ist. Mit (1.15.) und (1.30.) folgt $\text{Ke}(\text{tr}_R^{A_1}) = \underline{\det}_R^{C_2}(A_1) = \underline{\det}_R^G(A)$. A besitzt also eine Zerlegung $A = R \cdot b \oplus \underline{\det}_R^G(A) \oplus \text{Ke}(\pi)$.

(1.38). Proposition. Sei $R \hookrightarrow A$ eine C_2^a -Galois-erweiterung, $a \geq 1$. Ist R zusammenhängend (d.h. R hat keine Idempotente außer 0 und 1) und A nicht-zusammenhängend, so ist $\det_R^{C_2^a}([A]) = [R]$.

Beweis. Villamayor und Zelinsky [42] haben gezeigt, daß in diesem Fall eine zusammenhängende Galoiserweiterung $R \hookrightarrow S$ und ein $n \in \mathbb{N}$ existieren, so daß $A \cong S^n$ isomorphe R -Algebren sind. Man sieht, daß n dann ein Teiler von 2^a ist. Ist $n \cdot m = 2^a$, so gilt

$$\det_R^{C_2^a}([A]) = [\wedge_R^{2^a} (\bigoplus_n S)] = [\bigotimes_n \wedge_R^m(S)] = [\wedge_R^m(S)]^n.$$

Nun ist aber $\wedge_R^m(S)$ die Determinante einer Galoiserweiterung. Da n gerade ist, folgt aus (1.25) $\det_R^{C_2^a}([A]) = [R]$.

§ 5 Invarianten abelscher Galoiserweiterungen

(1.39.) Definitionen. Für eine endliche abelsche Gruppe G hat Harrison [26] auf $\text{Gal}(R, G)$ eine abelsche Gruppen-

struktur definiert. Wir wollen sie kurz andeuten.

Δ bezeichne die Untergruppe $\{(g, g^{-1}) \mid g \in G\} \hookrightarrow G \times G$.

Für $A, B \in \text{Gal}(R, G)$ ist $A \otimes B$ mit komponentenweiser Operation eine $(G \times G)$ -Galoiserweiterung. Der Fixring $(A \otimes B)^\Delta$ ist eine G -Galoiserweiterung mit der Operation

$$g(a \otimes b) = (ga) \otimes b = a \otimes (gb). \quad [A][B] := [(A \otimes B)^\Delta]$$

ist die Verknüpfung in $\text{Gal}(R, G)$. Das neutrale Element hat als Repräsentant die duale Gruppenalgebra $R[G]^*$ mit der

G -Struktur $(hv)(g) := v(gh)$ für $g, h \in G$ und $v \in R[G]^*$.

Der Repräsentant A^{-1} für das Inverse von A stimmt als

R -Algebra mit A überein. Die G -Struktur von A^{-1} ist

mit derjenigen von A durch folgende Gleichung verknüpft:

$$g * a = g^{-1}(a), \quad g \in G, \quad a \in A = A^{-1}.$$

Läßt man im zweiten Argument des Funktors $\text{Gal}(-, -)$ (vgl.

1.2.) nur abelsche Gruppen zu, so erhält man einen

Funktor $\underline{R} \times \underline{f\text{-Ab}} \longrightarrow \underline{Ab}$ (vgl. [26]).

Die Gruppenstruktur auf $\text{Pic}(R)$ ist allgemein bekannt.

In Ergänzung von (1.21.) wollen wir aber die Struktur von

$\text{Dis}(R)$ skizzieren. Das Tensorprodukt von Diskriminantenmoduln ist durch

$$(P, \alpha) \otimes (P', \alpha') := (P \otimes P', \alpha \otimes \alpha') \quad \text{und}$$

$$\alpha \otimes \alpha' (x \otimes x', y \otimes y') := \alpha(x, y) \alpha'(x', y') \quad \text{definiert.}$$

Für $(P, \alpha) \in \underline{\text{Dis}}(R)$ sind $(P, \alpha) \otimes (R, 1) \simeq (P, \alpha)$ und

$\alpha : (P, \alpha) \otimes (P, \alpha) \xrightarrow{\sim} (R, 1)$ Isomorphismen von Dis -

kriminantenmoduln. Auf die Isomorphieklassen übertragen ergibt dies auf $\text{Dis}(R)$ eine abelsche Gruppenstruktur vom Exponent 2. $[R, 1]$ ist das neutrale Element (vgl. [7] S.164).

(1.40.) Proposition. Für einen kommutativen Ring R und eine endliche abelsche Gruppe G sind die Invarianten $\text{dis}_R^G : \text{Gal}(R, G) \longrightarrow \text{Dis}(R)$ und $\text{det}_R^G : \text{Gal}(R, G) \longrightarrow \text{Pic}(R)$ mit den Gruppenstrukturen verträglich.

Beweis. Für quadratische Erweiterungen hat Revoy gezeigt, daß $\text{dis}_R^{C^2}$ ein Homomorphismus ist ([36] S.314). Ist $\text{sign}_R^G = 1$, so schickt dis_R^G alles auf das neutrale Element $[R, 1]$ (1.25.). Ist $\text{sign}_R^G \neq 1$, so sind wir in der Situation von (1.29.), und die Gleichung $\text{dis}_R^G = \text{dis}_R^{C^2} \text{Gal}(R, \text{sign}_R^G)$ zeigt, daß dis_R^G ein Homomorphismus ist.

Vergleicht man die Gruppenstrukturen von $\text{Dis}(R)$ und $\text{Pic}(R)$, so sieht man, daß der Vergißfunktorkomorphismus $\text{vergiß} : \text{Dis}(R) \ni [P, \alpha] \longrightarrow [P] \in \text{Pic}(R)$ induziert. Deshalb ist auch $\text{det}_R^G = \text{vergiß} \circ \text{dis}_R^G$ ein Homomorphismus.

(1.41.) Definition. Für abelsche G -Galoiserweiterungen $R \hookrightarrow A$ haben Garfinkel und Orzech gezeigt: A ist als Modul über dem (kommutativen) Gruppenring $R[G]$ endlich erzeugt projektiv vom Rang 1, und die Zuordnung

$\text{pic}_R^G : \text{Gal}(R, G) \longrightarrow \text{Pic}(R[G])$, $[A] \longmapsto [A]$ ist
mit den Gruppenstrukturen verträglich [23, 35].
Childs und Magid [16] nennen sie Picard-Invariante.

(1.42.) Satz. Für einen kommutativen Ring R und
eine endliche abelsche Gruppe G sind die drei In-
varianten durch folgendes kommutative Diagramm
abelscher Gruppen und Homomorphismen verknüpft

$$\begin{array}{ccc} \text{Gal}(R, G) & \xrightarrow{\text{pic}_R^G} & \text{Pic}(R[G]) \\ \text{dis}_R^G \downarrow & \searrow \text{det}_R^G & \downarrow \text{sign}^* \\ \text{Dis}(R) & \xrightarrow{\text{vergi\ss}} & \text{Pic}(R). \end{array}$$

sign^* bezeichnet dabei den durch sign^+) induzierten
Induktionsfaktor $[A] \longmapsto [A \otimes_{R[G]}^{\text{sign}^R} \text{sign}^R]$.

Beweis. Daß das untere Dreieck kommutiert, haben wir
schon bei (1.40.) bemerkt. Für die Kommutativität des
oberen Dreiecks ist zu zeigen, daß $A \otimes_{R[G]}^{\text{sign}^R} \text{sign}^R \simeq A^{\text{sign}}$
isomorphe R -Moduln sind.

Als ersten Schritt zeigen wir dazu, daß die Zuordnung
 $\pi : A \longrightarrow A^{\text{sign}}, a \longmapsto \sum_{g \in G} \text{sign}(g) \cdot g(a)$ ein surjek-
tiver $R[G]$ -Homomorphismus ist, wenn $R[G]$ auf A^{sign}
via sign operiert.

^{*)} Im nun folgenden Beweis schreiben wir statt sign_R^G
einfach sign .

π ist wohldefiniert, denn für $a \in A$ und $h \in G$ ist

$$\begin{aligned} & h \left(\sum_{g \in G} \text{sign}(g) \cdot g(a) \right) \\ &= \text{sign}(h) \left(\sum_{g \in G} \text{sign}(h) \cdot \text{sign}(g) \cdot hg(a) \right) \\ &= \text{sign}(h) \left(\sum_{g \in G} \text{sign}(g) \cdot g(a) \right). \end{aligned}$$

Die R -Linearität ist klar. Und die Gleichung $\pi(ha) = \sum_{g \in G} \text{sign}(g) \cdot g(ha) = \sum_{g \in G} \text{sign}(g) \cdot hg(a) = h\pi(a)$ zeigt, daß π auch die G -Struktur respektiert. Zum Nachweis der Surjektivität betrachten wir das Diagramm

$$\begin{array}{ccc} A \otimes_R A^{\text{sign}} & \xrightarrow{\pi \otimes A^{\text{sign}}} & A^{\text{sign}} \otimes_R A^{\text{sign}} \\ \text{mult} \downarrow \wr & & \downarrow \wr \text{mult} \\ A & \xrightarrow{\text{tr}_R^A} & A^G. \end{array}$$

Die senkrechten Pfeile sind bijektiv (vgl. 1.13., 1.23.); der Spurmorphismus ist surjektiv (vgl. 1.1.); und für $a \otimes b \in A \otimes_R A^{\text{sign}}$ ist

$$\begin{aligned} & \text{mult } \pi \otimes A^{\text{sign}}(a \otimes b) \\ &= \pi(a) \cdot b = \sum_{g \in G} \text{sign}(g) \cdot g(a) \cdot b = \\ &= \sum_{g \in G} (\text{sign}(g) \cdot b) \cdot g(a) = \sum_{g \in G} g(ab) = \\ &= \text{tr}_R^A(\text{mult}(a \otimes b)). \end{aligned}$$

Also ist $\pi \otimes A^{\text{sign}}$ ein Epimorphismus. Da der R -Modul A^{sign} treuprojektiv ist, ist π surjektiv.

Der Funktor $\text{sign}^* = - \otimes_{R[G]} \text{sign}^R : \underline{R[G]\text{-Mod}} \longrightarrow \underline{R\text{-Mod}}$

ist linksadjungiert zum Vergißfunktor $\underline{R\text{-Mod}} \longrightarrow \underline{R[G]\text{-Mod}}$,
der einen R -Modul M mit der $R[G]$ -Struktur via sign
versieht. sign^* erhält deshalb Epimorphismen.

Auf π angewendet ergibt sign^* also einen surjektiven
 R -Homomorphismus

$$\text{sign}^*(A) = A \otimes_{R[G]} \text{sign}^R \xrightarrow{\text{sign}^*(\pi)} A^{\text{sign}} \otimes_{R[G]} \text{sign}^R \simeq A^{\text{sign}}.$$

Da beide R -Moduln endlich erzeugt projektiv vom Rang 1
sind, ist dies sogar ein Isomorphismus.

(1.43.) Bemerkung. Die Aussage über die Kommutativität
des oberen Dreiecks in Satz (1.42.) verallgemeinert ein
Resultat von Childs und Magid. Sie haben dies für quadra-
tische Erweiterungen gezeigt, unter der Voraussetzung,
daß 2 in R ein Nicht-Nullteiler ist ([16] Prop.3.2.).
Bei ihrem Beweis geht die Bedingung "2 ist Nicht-Null-
teiler" entscheidend ein. Insofern ist unser Beweis von
(1.42.) auch im quadratischen Fall von Interesse.

§ 6 Modulstrukturen von Galoiserweiterungen mit zyklischen Galoisgruppen von 2-Potenz-Ordnung

Über die Modulstrukturen von G -Galoiserweiterungen eines
Ringes R mit Serre-Dimension 1 wissen wir inzwischen:

Ist $\text{sign}_R^G = 1$, so sind alle G-Galoiserweiterungen frei, und ist $\text{sign}_R^G \neq 1$, dann besitzt G eine von 0 verschiedene zyklische 2-Sylowuntergruppe H, und für G-Galoiserweiterungen sind bis auf freie direkte Summanden dieselben R-Modulstrukturen möglich wie für H-Galoiserweiterungen (1.26.).

Um zu wissen, welche Modulstrukturen bei Galoisweiterungen von R auftreten, genügt es daher die Bilder der Determinanten $\det_R^{C_{2^n}}$ zu kennen.

(1.44.) Satz. Für einen kommutativen Ring R ergeben die Bilder der Determinanten zu den zyklischen Gruppen von 2-Potenzordnung eine absteigende Kette abelscher Gruppen vom Exponent 2

$$\text{Bi}(\det_R^{C_2}) \supseteq \dots \supseteq \text{Bi}(\det_R^{C_{2^n}}) \supseteq \text{Bi}(\det_R^{C_{2^{n+1}}}) \supseteq \dots$$

Beweis. Da die Determinanten im abelschen Fall Homomorphismen sind (1.40.), sind die $\text{Bi}(\det_R^{C_{2^n}})$ Untergruppen von $\text{Pic}(R)$. Aus (1.25.) wissen wir auch schon, daß sie Exponent 2 haben. Daß sie in der angegebenen Weise ineinander enthalten sind, folgt aus (1.30.).

Die Kette

$\text{Bi}(\det_R^{C_2}) \supseteq \dots \supseteq \text{Bi}(\det_R^{C_{2^n}}) \supseteq \text{Bi}(\det_R^{C_{2^{n+1}}}) \supseteq \dots$ besteht aus $\text{GF}(2)$ -Vektorräumen. Die für uns interessanten Eigenschaften sind offensichtlich die $\text{GF}(2)$ -Dimensionen von

$\text{Bi}(\det_R^{C_{2^n}})$, $n \geq 1$ und

von $\text{Bi}(\det_R^{C_{2^n}}) / \text{Bi}(\det_R^{C_{2^{n+1}}})$, $n \geq 1$.

Sie beschreiben für einen Ring R der Serre-Dimension 1 die Anzahl der möglichen R -Modulstrukturen von C_{2^n} -Galoiserweiterungen und die Anzahl der Modulstrukturen $[M] = [R^{2^n-1} \oplus \wedge_R^{2^n}(M)]$, welche bei C_{2^n} -Galoiserweiterungen auftreten, deren entsprechende Struktur $[R^{2^{n+1}-1} \oplus \wedge_R^{2^{n+1}}(M)]$ aber bei den $C_{2^{n+1}}$ -Galoiserweiterungen nicht vorkommt.

Im folgenden beschäftigen wir uns mit der Frage:
Welche Eigenschaften haben diese Ketten? Anders ausgedrückt: Welche "Typen" von Ketten kommen auf die in (1.44.) beschriebene Weise zustande?

(1.45.) Bezeichnungen und Definition.

$$B_n(R) := \text{Bi}(\det_R^{C_{2^n}}), \quad n \geq 1$$

$$\mathcal{L}(R) := (B_1(R) \supseteq B_2(R) \supseteq \dots \supseteq B_n(R) \supseteq \dots)$$

$$b_n(R) := \text{GF}(2) - \dim(B_n(R)), \quad n \geq 1$$

$$d_n(R) := \text{GF}(2) - \dim(B_n(R) / B_{n+1}(R)), \quad n \geq 1$$

Das Folgenpaar $((b_n(R)), (d_n(R)))$ nennen wir den "Typ" der Kette $\mathcal{L}(R)$.

Offensichtlich genügen die so definierten Kardinalzahlen $d_n(R)$, $b_n(R)$ den Gleichungen $b_n(R) = d_n(R) + b_{n+1}(R)$, $n \geq 1$. Die Gültigkeit dieser Gleichungen ist also eine notwendige Bedingung dafür, daß ein Folgenpaar von Kardinalzahlen $(b_i), (d_i)$ als "Typ" einer Kette $\mathcal{L}(R)$ auftreten kann. Überraschenderweise zeigt sich, daß diese Bedingung auch hinreichend ist.

(1.46.) Theorem. Seien $(b_i)_{i \in \mathbb{N}}$, $(d_i)_{i \in \mathbb{N}}$ Folgen von Kardinalzahlen, welche die Gleichungen $b_i = d_i + b_{i+1}$, $i \in \mathbb{N}$ erfüllen. Dann gibt es einen Dedekindring R , dessen Kette $\mathcal{L}(R)$ vom Typ $((b_i), (d_i))$ ist.

(1.47.). Dieses Resultat rundet unsere Ergebnisse von Kapitel 1 ab. Um entscheiden zu können, welche Modulstrukturen bei Galoiserweiterungen eines Ringes der Serre-Dimension 1 auftreten, schien es zunächst nötig zu sein, für alle endlichen Gruppe G die Teilmengen $Bi(\det_R^G) \subseteq \text{Pic}(R)$ zu bestimmen. Doch dann zeigte sich, daß man sich dabei auf die Gruppen C_{2^n} , $n \geq 1$ beschränken kann. Eine weitere Einschränkung ist allerdings nicht mehr möglich, wie Theorem (1.46.) zeigt.

Nun drängt sich natürlich sofort folgende Frage auf:
Welche Eigenschaften charakterisieren die Elemente
der Untergruppen $\text{Bi}(\det_R^{C_{2^n}}) \hookrightarrow \text{Pic}(R)$?

Im quadratischen Fall wurde diese Frage von C. Small
[38] gelöst. Er gibt dazu die exakte Folge an

$$0 \longrightarrow \mathcal{F}(R) \longrightarrow \mathcal{Q}(R) \xrightarrow{\det_R^{C_2}} \text{Pic}_{(2)}(R) \longrightarrow U'(R)$$

(vgl. Kapitel 3, Anhang). Für den allgemeinen Fall
müssen wir diese Frage offen lassen, für spezielle
Ringe bieten wir jedoch eine Lösung an. Dieses Er-
gebnis werden wir auch beim Beweis von (1.46.) be-
nutzen.

Bezeichnung. Für eine abelsche Gruppe G und eine
natürliche Zahl n sei $G[n]$ die Untergruppe der von
 n annullierten Elemente.

(1.48.) Satz. Sei R ein zusammenhängender kommutativer
Ring, der $\frac{1}{2}$ enthält und primitive 2^n -te Einheitswurzeln
für alle $n \geq 1$. Dann gilt für alle $n \geq 1$

$$\text{Bi}(\det_R^{C_{2^n}}) = \{ [P] \in \text{Pic}(R) \mid [P] \text{ wird von } 2 \text{ annulliert und ist durch } 2^{n-1} \text{ teilbar} \}.$$

Beweis von (1.48.). Als wesentliches Hilfsmittel be-
nutzen wir folgendes Resultat von Childs ([14] Theorem 9):

Unter den Voraussetzungen des Satzes ist die Charaktergruppe $\text{Grp} (C_{2^n}, U(R))$ zu C_{2^n} isomorph. Ist χ ein erzeugendes Element davon, so ist eine C_{2^n} -Galoiserweiterung $R \hookrightarrow A$ als $R[C_{2^n}]$ -Modul isomorph zu $\bigoplus_{j=1}^{2^n} (A^\chi)^j \cong \bigoplus_{j=1}^{2^n} A(\chi^j)$. Die C_{2^n} -Struktur ist dabei

$$g(\sum_j a_j) = \sum_j \chi^j(g) a_j, \quad g \in C_{2^n}, \quad a_j \in A(\chi^j).$$

Childs zeigt außerdem, daß das Bild der Zuordnung $\text{Gal}(R, C_{2^n}) \ni [A] \longmapsto [A^\chi] \in \text{Pic}(R)$ gleich $\text{Pic}(R)[2^n] = \{ [P] \in \text{Pic}(R) \mid [P] \text{ wird von } 2^n \text{ annulliert} \}$ ist.

Die Aussage von (1.48.) ergibt sich daraus durch folgende Überlegungen:

Es ist $\chi^{2^{n-1}} = \text{sign}_R^{C_{2^n}}$. Also kommutiert das Diagramm

$$\begin{array}{ccc} \text{Gal}(R, C_{2^n}) & \xrightarrow{[(-)^\chi]} & \text{Pic}(R)[2^n] \\ \searrow \det_R^{C_{2^n}} & & \swarrow (-)^{2^{n-1}} \\ & \text{Pic}(R). & \end{array}$$

Da der horizontale Pfeil surjektiv ist, folgt

$$\begin{aligned} \text{Bi}(\det_R^{C_{2^n}}) &= \{ [P]^{2^{n-1}} \in \text{Pic}(R) \mid [P] \in \text{Pic}(R)[2^n] \} \\ &= \{ [P] \in \text{Pic}(R) \mid [P] \in \text{Pic}(R)[2] \text{ und } [P] \text{ ist durch } 2^{n-1} \text{ teilbar} \}. \end{aligned}$$

Beweis von Satz (1.47.). Aus (1.48.) sieht man, daß

es genügt, einen Dedekindring R zu finden, der $\frac{1}{2}$ und primitive 2^n -te Einheitswurzeln für alle $n \geq 1$ enthält, und dessen Picardgruppe folgender Bedingung genügt: die Untergruppen $\text{Pic}(R)[2] \cap 2^{n-1} \text{Pic}(R)$ bilden eine absteigende Kette vom vorgegebenen Typ. Nun besagt der Satz von Claborn: Für jede abelsche Gruppe G existiert ein Dedekindring R mit $\text{Pic}(R) \simeq G$ ([18] Chap. 3, Theorem 14.10.).

Verfolgt man Fossums Beweis, so stellt man fest, daß in Claborns Satz der Ring R immer so gewählt werden kann, daß er $\mathbb{C}$ als Unterring enthält.

(Für $G \simeq \mathbb{Z}^{(S)}/H$ gibt ([18] 14.8.) einen Krullring $R'' = \mathbb{C}^{(S)} \hookrightarrow \mathbb{C}$ an mit $\text{Cl}(R'') \simeq \mathbb{Z}^{(S)}$; ([18] 14.4.) zeigt die Existenz eines Krullrings R' mit $R' \hookrightarrow R'' \hookrightarrow \mathbb{C}$ und $\text{Cl}(R') \simeq G$; ([18] 14.2.) ergibt schließlich einen Dedekindring R mit $R \hookrightarrow R' \hookrightarrow R'' \hookrightarrow \mathbb{C}$ und $\text{Pic}(R) \simeq \text{Cl}(R) \simeq \text{Cl}(R') \simeq G$.)

Es genügt also eine abelsche Gruppe G anzugeben, deren Untergruppen $G[2] \cap 2^{n-1}G$, $n \geq 1$ eine absteigende Kette vom Typ $((b_1), (d_1))$ bilden. Die Existenz einer solchen Gruppe G zeigen wir im nachfolgenden Hilfssatz und haben dann auch Satz (1.47.) bewiesen.

(1.49.) Hilfssatz. Seien $(b_i)_{i \in \mathbb{N}}$, $(d_i)_{i \in \mathbb{N}}$ Folgen von Kardinalzahlen, und es gelte für alle $i \in \mathbb{N}$: $b_i = d_j + b_{i+1}$. Dann gibt es eine abelsche Gruppe G , deren absteigende Kette von Untergruppen $G_n := G[2] \cap 2^{n-1}G$, $n \in \mathbb{N}$ folgende Eigenschaften hat

$$a.) \dim_{GF(2)} (G_i / G_{i+1}) = d_i, \quad i \in \mathbb{N}$$

$$b.) \dim_{GF(2)} (G_i) = b_i, \quad i \in \mathbb{N}.$$

Beweis. Die Menge der Kardinalzahlen $\{b_i \mid i \in \mathbb{N}\}$ ist wohlgeordnet. Sei b_ω ihr kleinstes Element. Sei ferner $J := \{i \in \mathbb{N} \mid b_i = b_\omega\}$ und j das kleinste Element der nicht-leeren Menge J . Aus den Relationen $b_i = d_i + b_{i+1}$ folgt: für $i \geq j$ ist $b_i = b_\omega$, für $i < j$ ist $b_i = b_\omega + d_{j-1} + \dots + d_i$. Ist b_ω endlich, so ist $d_i = 0$ für $i \geq j$. Falls b_ω unendlich ist, dann folgt nur $d_i \leq b_\omega$ für $i \geq j$.

Nun konstruieren wir G . Seien

$$V_i := C_2^{i(d_i)}, \quad i \in \mathbb{N}$$

$$V_\omega := \mathbb{Z}(2^\infty)^{(b_\omega)}$$

$$G := \bigoplus_{i=1}^{\omega} V_i.$$

Dann gelten $G[2] = \bigoplus_{i=1}^{\omega} V_i[2]$; $V_i[2] \simeq C_2^{(d_i)}$, $i \in \mathbb{N}$;

$V_\omega[2] \simeq C_2^{(b_\omega)}$. Für $n \in \mathbb{N}$ ist $G_n = G[2] \cap 2^{n-1}G =$

⁺) Damit ist das Koproduct von d_i Kopien von C_2 gemeint.

$\bigoplus_{i=n}^{\omega} V_i[2]$ und $G_n/G_{n+1} = V_n[2] \cong C_2^{(d_n)}$. Die

Bedingung a.) ist also erfüllt.

Um b.) nachzuweisen, machen wir die Vorüberlegung

$b_{\omega} + \sum_{i \geq j} d_i = b_{\omega}$. Ist b_{ω} endlich, so ist dies klar, da $d_i = 0$ ist, für $i \geq j$. Ist b_{ω} unendlich, so gilt

$$b_{\omega} \leq b_{\omega} + \sum_{i \geq j} d_i \leq b_{\omega} + \sum_{i \geq j} b_{\omega} = b_{\omega} + \aleph_0 b_{\omega} = b_{\omega}.$$

Damit zeigen wir nun $\dim_{GF(2)} = b_n$, $n \in \mathbb{N}$. Für $n \geq j$

$$\text{ist } \dim_{GF(2)} G_n = b_{\omega} + \sum_{i \geq n} d_i \leq b_{\omega} + \sum_{i \geq j} d_i = b_{\omega} = b_n.$$

Sei nun $n < j$. Dann ist

$$\begin{aligned} \dim_{GF(2)} G_n &= b_{\omega} + \sum_{i \geq n} d_i = \sum_{i=n}^{j-1} d_i + \dim_{GF(2)} G_j = \\ d_n + \dots + d_{j-1} + b_{\omega} &= b_n. \end{aligned}$$

Kapitel 2

KOHOMOLOGISCHE BESCHREIBUNGEN DER INVARIANTEN VON GALOISERWEITERUNGEN

In diesem Kapitel sollen die kohomologischen Hilfsmittel für Kapitel 3 bereitgestellt werden. Kohomologische Beschreibungen der Invarianten quadratischer Erweiterungen werden dort eine zentrale Rolle spielen. Obwohl diese Ergebnisse von technischer Natur sind, scheinen sie mir interessant genug, um sie, über den quadratischen Fall hinausgehend, für beliebige Galoiserweiterungen darzustellen.

Unser wichtigstes Werkzeug wird Grothendiecks [24] Theorie verzerrter Formen sein. Bei ihr geschieht der Übergang zu Amitsurscher und Čechscher Kohomologie auf sehr anschauliche Weise. Leider existiert davon in der Literatur keine für unsere Zwecke geeignete Darstellung. Deshalb entwickeln wir zu Beginn dieses Kapitels die Technik der verzerrten Formen soweit wir sie benötigen.

(2.1.) Bezeichnungen. Ergänzend zu Kapitel 1 § 0 notieren wir: $\underline{\text{Me}}^*$ sei die Kategorie der punktierten Mengen. Ihre Morphismen sind Abbildungen, welche die ausgezeichneten Punkte ineinander überführen. Für die Kategorie der treuflachen R-Algebren und R-Algebren-

homomorphismen schreiben wir R-Alg-tf .

Sind $F : \underline{R\text{-Alg}} \longrightarrow \underline{Me}^*$ ein Funktor und

$\eta : R \longrightarrow S$ eine R-Algebra, so sei

$F(S/R) := \{ x \in F(R) \mid F(\eta)(x) = * \}$. * steht

dabei für den ausgezeichneten Punkt von $F(S)$.

Für einen Homomorphismus kommutativer Ringe $d : S \longrightarrow T$

bezeichnen wir mit ${}_d T$ den S-Modul T, auf dem S via

d operiert. Für den "Induktionsfunktor"

$- \otimes_S ({}_d T) : \underline{S\text{-Mod}} \longrightarrow \underline{T\text{-Mod}}$ schreiben wir d^* . (Dies ist konsistent mit der in (1.42.) benutzten Bezeichnung sign^* .)

§ 1 Verzernte Formen

Die Theorie der verzernten Formen ist im wesentlichen ein Teil von Grothendiecks treuflacher Abstiegstheorie [24]. Er formulierte sie jedoch in so großer Allgemeinheit, daß es in unserer Situation weniger anstrengend ist, die Theorie neu zu entwickeln, als seine Ergebnisse zu konkretisieren. Die Darstellung von Knus und Ojanguren [29] kommt unseren Bedürfnissen sehr viel näher, ist aber letztlich doch zu speziell.

Worum es sich handelt, soll zunächst an zwei Beispielen aufgezeigt werden.

(2.2.) Beispiel. (vgl. [29]S.63) Sei $R \hookrightarrow S$ eine treuflache Erweiterung, und sei M ein R -Modul. Eine Isomorphieklasse $[N]$ von R -Moduln heißt verzerrte Form von M bezüglich S , wenn die S -Moduln $M \otimes S$ und $N \otimes S$ isomorph sind.

Die Menge der verzerrten Formen von M entspricht bijektiv der Amitsurschen Kohomologiemenge $H^1(S/R, \underline{\text{Aut}} M)$. Dabei bezeichnet $\underline{\text{Aut}} M$ den Funktor, welcher einer R -Algebra T die Gruppe der T -Modul-Automorphismen von $M \otimes T$ zuordnet. Im Spezialfall $M = R$ ergibt sich auf diese Weise der bekannte Isomorphismus $\text{Pic}(S/R) \simeq H^1(S/R, U)$ (vgl. [13, 17, 29]).

Die bijektive Zuordnung zwischen der Menge verzerrter Formen und einer Amitsurschen Kohomologiemenge läßt sich auch dann noch angeben, wenn man Moduln betrachtet, die eine zusätzliche Struktur tragen.

(2.3.) Beispiel. Betrachtet man verzerrte Formen von G -Galoiserweiterungen, so lauten die modifizierten Begriffe folgendermaßen: Ist $R \hookrightarrow S$ treuflach und $A \in \underline{\text{Gal}}(R, G)$, so heißt $[B] \in \underline{\text{Gal}}(R, G)$ verzerrte Form von A bezüglich S , wenn $A \otimes S$ und $B \otimes S$ in $\underline{\text{Gal}}(S, G)$ isomorph sind. Der Funktor $\underline{\text{Aut}} A$ ordnet in diesem Fall einer R -Algebra T die Gruppe der $\underline{\text{Gal}}(T, G)$ -Automorphismen von $A \otimes T$ zu. Die Bijektion zwischen der Menge der verzerrten Formen von A bezüglich S und $H^1(S/R, \underline{\text{Aut}} A)$

ergibt im Spezialfall der trivialen G-Galoiserweiterung $R[G]^*$ eine kohomologische Beschreibung von $\text{Gal}(\mathbb{S}/R, G)$ (vgl. 2.17.).

Da wir entsprechende Aussagen für eine ganze Reihe von Strukturtypen benötigen, wollen wir einen Beweis von hinreichender Allgemeinheit geben. Dabei nehmen wir in Kauf, daß der Begriffsapparat des "abstrakten Strukturtyps" den gesamten Beweisablauf schwerfälliger macht. Die Beweisidee hingegen ist nicht anders als etwa im Fall von Galoiserweiterungen.

Im vorliegenden Paragraphen wird zunächst nur ein abstrakter Strukturbegriff eingeführt, und verzerrte Formen und Automorphismen-Funktoren werden in diesem Kontext formuliert. Die bijektive Zuordnung zwischen Isomorphieklassen und Kohomologieklassen behandeln wir anschließend in einem gesonderten Abschnitt.

Für unsere Zwecke genügt es, wenn wir Strukturtypen betrachten, die sich durch eine Menge von Pfeilen $x \xrightarrow{\varphi} y$ beschreiben lassen. Auf der Pfeil-Menge braucht keine Verknüpfung definiert zu sein. Deshalb erinnern wir an den Begriff eines gerichteten Graphen.

(2.4.) Definition. Ein gerichteter Graph $\underline{A}$ ist ein Quadrupel $(\dot{A}, \vec{A}, Q, Z)$. $\dot{A}$ und $\vec{A}$ sind dabei Mengen, deren Elemente "Punkte" bzw. "Pfeile" genannt werden.

Q und Z sind Abbildungen $\vec{A} \longrightarrow \dot{A}$; sie ordnen einem Pfeil seine "Quelle" und sein "Ziel" zu. Wie in einer Kategorie schreiben wir " $x \xrightarrow{\varphi} y$ ", um auszudrücken, daß φ ein Pfeil mit Quelle x und Ziel y ist.

Ein Morphismus $\underline{F} : \underline{A} \longrightarrow \underline{B}$ gerichteter Graphen ist ein Paar $\vec{F} : \vec{A} \longrightarrow \vec{B}$, $\dot{F} : \dot{A} \longrightarrow \dot{B}$, welches Quelle und Ziel der Pfeile respektiert. Folgendes Diagramm muß also kommutieren

$$\begin{array}{ccc} \vec{A} & \xrightarrow{\vec{F}} & \vec{B} \\ Q \downarrow & & \downarrow Z \\ \dot{A} & \xrightarrow{\dot{F}} & \dot{B} \end{array} .$$

(2.5.) Definition zulässiger Strukturen.

(2.5.1.) Eine zulässige Struktur $\underline{A}$ besteht aus einem gerichteten Graphen $\underline{A}$, einer Familie von Funktoren $(F_x^S : \underline{S}\text{-Mod} \longrightarrow \underline{S}\text{-Mod} \mid x \in \dot{A}, S \in \underline{R}\text{-Alg})$ und einer Familie von funktoriellen Isomorphismen

$(\phi_x^q : F_x^S(-) \otimes_S T \xrightarrow{\sim} F_x^T(- \otimes_S T) \mid x \in \dot{A}; S, T \in \underline{R}\text{-Alg}; q \in \underline{R}\text{-Alg}(S, T))$, welche folgenden Verträglichkeitsbedingungen genügt

$$1.) \forall x \in \dot{A} \quad \forall S \in \underline{R}\text{-Alg} \quad \forall M \in \underline{S}\text{-Mod} :$$

$$\begin{array}{ccc} F_x^S(M) \otimes_S S & \xrightarrow{\phi_x^{\text{id}(M)}} & F_x^S(M \otimes_S S) \\ \text{kan} \searrow \sim & \parallel & \swarrow \sim \\ & F_x^S(M) & F_x^S(\text{kan}) \end{array}$$

ii.) $\forall x \in \dot{A} \quad \forall q \in \underline{R\text{-Alg}}(S, T) \quad \forall q' \in \underline{R\text{-Alg}}(T, T')$
 $\forall M \in \underline{S\text{-Mod}} :$

$$\begin{array}{ccc}
 (F_x^S(M) \otimes_S T) \otimes_T T' & \xrightarrow{\phi_x^{q(M)} \otimes T} & F_x^{T'}(M \otimes_S T) \otimes_T T' \\
 \downarrow \text{kan} \wr & \parallel & \downarrow \phi_x^{q'}(M \otimes_S T) \\
 F_x^S(M) \otimes_S T' & & F_x^{T'}(M \otimes_S T \otimes_T T') \\
 \searrow \phi_x^{q'} q(M) & & \swarrow \sim \\
 & F_x^{T'}(M \otimes_S T') & F_x^{T'}(\text{kan})
 \end{array}$$

(2.5.2.) Durch eine zulässige Struktur $\underline{A}$ ist für jede R -Algebra S eine Kategorie $\underline{A}_S$ gegeben. Objekte von $\underline{A}_S$ sind Paare $(A, \mathcal{A})$ aus einem S -Modul A und einem Morphismus gerichteter Graphen $\mathcal{A}: \underline{A} \longrightarrow \underline{S\text{-Mod}}$, so daß für jeden Punkt x aus A die Gleichung $\mathcal{A}(x) = F_x^S(A)$ gilt. Ein Morphismus $f: (A, \mathcal{A}) \longrightarrow (A', \mathcal{A}')$ in $\underline{A}_S$ ist ein S -Modulhomomorphismus $f: A \longrightarrow A'$, so daß für jeden Pfeil $\psi: x \longrightarrow y$ aus $\underline{A}$ folgendes Diagramm kommutiert

$$\begin{array}{ccc}
 \mathcal{A}(x) & \xrightarrow{\mathcal{A}(\psi)} & \mathcal{A}(y) \\
 \downarrow F_x^S(f) & & \downarrow F_y^S(f) \\
 \mathcal{A}'(x) & \xrightarrow{\mathcal{A}'(\psi)} & \mathcal{A}'(y) .
 \end{array}$$

(2.5.3.) Ist $d: S \longrightarrow T$ ein R -Algebrenhomomorphismus, so wird durch Skalarbereichs-Erweiterung aus einem

Objekt $(A, \mathcal{A}) \in \underline{A}_S$ ein Objekt $(d^*(A), d^*(\mathcal{A})) \in \underline{A}_T$.

Dabei ist $d^*(A) = A \otimes_S d^T$ (vgl. 2.1.), und für

$\varphi : x \longrightarrow y$ ist $d^*(\mathcal{A})(\varphi)$ durch folgendes kommutative Diagramm bestimmt

$$\begin{array}{ccc} F_x^T(A \otimes_S T) & \xrightarrow{d^*(\mathcal{A})(\varphi)} & F_y^T(A \otimes_S T) \\ \downarrow \wr & & \downarrow \wr \\ F_x^S(A) \otimes_S T & \xrightarrow{\mathcal{A}(\varphi) \otimes_S T} & F_y^S(A) \otimes_S T. \end{array}$$

Ist $(A, \mathcal{A}) \in \underline{A}_R$ und $\eta : R \longrightarrow S$ der Eins-Morphismus, so schreiben wir statt $(\eta^*(A), \eta^*(\mathcal{A}))$ auch $(A_S, \mathcal{A}_S)$.

Man überzeugt sich leicht, daß für einen Morphismus

$f \in \underline{A}_S$ $((A, \mathcal{A}), (A', \mathcal{A}'))$ durch $d^*(f) = f \otimes_S d^T$

ein Morphismus $(d^*(A), d^*(\mathcal{A})) \longrightarrow (d^*(A'), d^*(\mathcal{A}'))$

in $\underline{A}_T$ gegeben ist. Damit ist $d^* : \underline{A}_S \longrightarrow \underline{A}_T$ der

Funktor "Skalarbereichs-Erweiterung längs d ".

Routineüberlegungen zeigen, daß bis auf funktorielle

Isomorphie id^* mit dem identischen Funktor und $(dd')^*$

mit $d^*d'^*$ übereinstimmen.

Machen wir uns das bisher Gesagte an einem Beispiel klar.

(2.6.) Die zulässige Struktur zur Beschreibung von G-Galoiserweiterungen.

Für eine endliche Gruppe G liegt den G-Galoiserwei-

terungen offensichtlich folgende zulässige Struktur $\underline{G}$ zugrunde:

Ihr Graph $\underline{G}$ besteht aus den Punkten 0, 1, 2 und den Pfeilen $\nabla : 2 \rightarrow 1$, $\eta : 0 \rightarrow 1$, $g : 1 \rightarrow 1$ für $g \in G$. Für eine R-Algebra T, einen T-Modul M und einen T-Modulhomomorphismus f ist

$$F_0^T(M) = T, F_0^T(f) = \text{id}$$

$$F_1^T(M) = M, F_1^T(f) = f$$

$$F_2^T(M) = M \otimes_T M, F_2^T(f) = f \otimes_T f.$$

Die funktoriellen Isomorphismen Φ sind die kanonischen.

Für eine R-Algebra T besteht die Kategorie $\underline{G}_T$ aus T-Moduln A mit einer Multiplikation $\nabla : A \otimes_T A \rightarrow A$, einem ausgezeichneten Element $1 \in A$ und einer Familie von T-Modulendomorphismen $g : A \rightarrow A$, $g \in G$. Morphismen sind T-Modulhomomorphismen, welche mit diesen Strukturabbildungen verträglich sind.

$\text{Gal}(T, G)$ ist eine volle isomorphie-abgeschlossene Unterkategorie von $\underline{G}_T$. $\text{Gal}(T, G)$ kann man daher als eine Menge von Isomorphieklassen in $\underline{G}_T$ auffassen.

(2.7.) Definition verzerrter Formen. Seien R ein kommutativer Ring, $\underline{A}$ eine zulässige Struktur und $(A, \mathcal{A}) \in \underline{A}_R$. S sei eine treuflache R-Algebra.

(2.7.1.) Eine verzerrte Form von $(A, \mathcal{A})$ bezüglich S ist eine Isomorphieklasse $[B, \mathfrak{B}]$ in $\underline{A}_R$, für welche $(A_S, \mathcal{A}_S) \simeq (B_S, \mathfrak{B}_S)$ in $\underline{A}_S$ isomorph sind. Soll die Struktur betont werden, so gebrauchen wir die Bezeichnung $\underline{A}$ -Form.

(2.7.2.) Ist S treuflach, so ist eine verzerrte Form von $(A, \mathcal{A})$ durch einen R -Untermodul $B \hookrightarrow A \otimes S$ und eine Familie $(\mathfrak{B}(\varphi))_{\varphi \in \underline{A}}$ mit $\mathfrak{B}(\varphi) \in R\text{-Mod}(F_X^R(B), F_Y^R(B))$ bestimmt. Es gibt also nur eine Menge verzerrter Formen von $(A, \mathcal{A})$ bezüglich S . Sie ist durch $[A, \mathcal{A}]$ punktiert. Wir schreiben dafür $V_{\underline{A}}^S(A, \mathcal{A})$ oder einfach $V_{\underline{A}}^S$, wenn klar ist, von welchem Objekt die $\underline{A}$ -Formen betrachtet werden.

(2.7.3.) Sind S, T treuflache R -Algebren und $d : S \longrightarrow T$ ein R -Algebrenhomomorphismus, so ist eine verzerrte Form $[B, \mathfrak{B}]$ von $(A, \mathcal{A})$ bezüglich S auch eine verzerrte Form bezüglich T , denn $\eta_{\mathfrak{T}}^*(B, \mathfrak{B}) \simeq d^* \eta_{\mathfrak{S}}^*(B, \mathfrak{B}) \simeq d^* \eta_{\mathfrak{S}}^*(A, \mathcal{A}) \simeq \eta_{\mathfrak{T}}^*(A, \mathcal{A})$.

$V_{\underline{A}}^d : V_{\underline{A}}^S \longrightarrow V_{\underline{A}}^T$ sei die Inklusion. Damit ist $V_{\underline{A}}$ ein Funktor $\underline{R}\text{-Alg-tf} \longrightarrow \underline{Me}^*$.

Auch dieser Begriff soll sogleich im Beispiel der G -Galoiserweiterungen betrachtet werden. Dabei deutet sich auch bereits an, warum für uns Mengen verzerrter Formen interessant sind.

Für einen kommutativen Ring R und eine endliche Gruppe G wollen wir die Menge $\text{Gal}(R, G)$ (vgl. 1.2.) durch verzerrte Formen der trivialen G -Galoiserweiterung $R[G]^*$ (vgl. 1.39) beschreiben. Dazu sehen wir uns zuerst deren Struktur genauer an.

(2.8.) Bezeichnungen. Die Basiselemente des Gruppenringes $R[G]$ bezeichnen wir mit u_g , $g \in G$. Die Elemente der dazu dualen Basis in $R[G]^*$ seien d_g , $g \in G$. In der R -Algebra $E_R^G = \underline{\text{Me}}(G, R)$ bilden die Elemente v_g , $g \in G$ mit $v_g(h) = \delta_{g,h}$ eine Basis, und E_R^G ist ein G -Linksmodul vermöge der Vorschrift

$$h \left(\sum_g r_g v_g \right) = \sum_g r_g v_{hg}, \quad h \in G.$$

(2.9.) Proposition. Die Zuordnungen

$$R[G] \xrightarrow{\alpha} E_R^G \xrightarrow{\alpha'} R[G]^*$$

$\sum_g r_g u_g \mapsto \sum_g r_g v_g \mapsto \sum_g r_g^{-1} d_g$ sind Isomorphismen von $R[G]$ -Moduln. α' ist außerdem ein Algebrenhomomorphismus, also ein Isomorphismus in $\text{Gal}(R, G)$.

Beweis. Die Abbildungen sind offensichtlich Isomorphismen von R -Moduln. Die G -Homogenität von α ist klar, für α' folgt sie aus

$$\begin{aligned} \alpha' \left(h \left(\sum_g r_g v_g \right) \right) (u_{g'}) & ; \quad h, g' \in G \\ &= \alpha' \left(\sum_g r_g v_{hg} \right) (u_{g'}) = \left(\sum_g r_g d_g^{-1} h^{-1} \right) (u_{g'}) \end{aligned}$$

$$= r_h^{-1} g'^{-1} = \left(\sum_g r_g d_g^{-1} \right) (u_{g',h})$$

$$= (h \alpha' \left(\sum_g r_g v_g \right)) (u_{g'}).$$

α' erhält außerdem die 1 und ist multiplikativ, denn die v_g und die d_g sind jeweils paarweise orthogonale Idempotente.

(2.10.) Proposition. Ist $R \hookrightarrow S$ treuflach, so stimmt $\text{Gal}(S/R, G)$ mit der Menge der $\underline{G}$ -Formen von E_R^G bezüglich S überein.

Beweis. Der kanonische Isomorphismus $E_S^G \simeq E_R^G \otimes S$ von S -Moduln ist ein $\text{Gal}(S, G)$ -Isomorphismus (vgl. [35] Lemma 1.4.). Eine Klasse $[A] \in \text{Gal}(S/R, G)$ ist also eine $\underline{G}$ -Form von E_R^G . Sei umgekehrt A ein Objekt in $\underline{E}_R^G$ mit Multiplikation ∇ , Einsmorphismus $\eta : R \longrightarrow A$ und Endomorphismen $g, g \in G$, so daß A_S zu E_S^G $\underline{G}_S$ -isomorph ist. Da die Diagramme, welche (A, ∇, η) als assoziative, kommutative R -Algebra mit Einselement ausweisen nach Tensorieren mit S kommutieren, kommutieren sie auch schon vorher. Die Endomorphismen $g_S : A_S \longrightarrow A_S$ sind bijektiv, paarweise verschieden, sie respektieren ∇_S und η_S , und es ist $e_S = \text{id}$ (e ist das neutrale Element der Gruppe G). Bezeichnen $\cdot$ die Verknüpfung der Gruppe G und $\circ$ die Komposition von Abbildungen, so gilt für $g, h \in G$ außerdem $(g \cdot h)_S = g_S \circ h_S$. Da S treuflach ist, übertragen sich all diese Eigenschaften auf die Endomorphismen $g : A \longrightarrow A$. Die Gruppe G operiert also auf der R -Algebra (A, ∇, η) durch R -Algebrenautomorphismen von links.

Die Erweiterung $R \hookrightarrow A$ ist treuflach, denn $S \hookrightarrow A_S$ ist treuflach (vgl. [10]Chap. 1, § 3, Prop. 6). Nach (1.1.a.) bleibt zu zeigen, daß $\theta : A \otimes A \longrightarrow E_A^G$ bijektiv ist. Orzech tut dies, indem er es für θ_S zeigt ([35] Lemma 1.5.).

(2.11.) Bemerkung. Beim Beweis von (2.10.) erkennt man, warum wir uns auf Strukturen beschränken können, deren Strukturmorphismen keinen Relationen genügen müssen : Relationen der Strukturhomomorphismen eines Objektes $(A, \mathcal{A})$, welche durch Diagramme beschreibbar sind, übertragen sich sowieso auf alle verzerrten Formen von $(A, \mathcal{A})$.

Nun wenden wir uns der Kohomologie zu, durch die wir die Mengen $V_{\underline{A}}^S$ beschreiben wollen. Die vorangegangenen Überlegungen im Fall von Galoiserweiterungen machen es klar, warum wir an einer solchen Beschreibung interessiert sind.

(2.12.) Definition der Amitsurschen Kohomologie.

Für eine R-Algebra S sei

$$R \longrightarrow S \xrightleftharpoons[d_2]{d_1} S \otimes S \xrightleftharpoons[d_3]{d_1} S \otimes S \otimes S \quad \dots$$

der Amitsursche Komplex $^+$). Die Morphismen d_i fügen

⁺) An dieser Stelle sei an unsere Konvention

$- \otimes -$ erinnert.
R

dabei an der i -ten Stelle eine 1 ein (vgl. [29] S. 119).

Ist $F : \underline{R\text{-Alg}} \longrightarrow \underline{Grp}$ ein Funktor und $k \in F(S \otimes \dots \otimes S)$, so kürzen wir $F(d_i)(k) = : k_i$ ab. Dabei wird jeweils aus dem Zusammenhang klar sein, welcher Funktor und welche Stelle des Amitsurschen Komplexes an der Bildung von k_i beteiligt waren.

Mit dieser Schreibweise heißt ein Element $k \in F(S \otimes S)$ 1-Kozykel, falls $k_2 = k_3 k_1$ ist. Zwei 1-Kozykeln k und k' heißen kohomolog, wenn ein $l \in F(S)$ existiert, so daß $k' = l_2 k l_1^{-1}$ ist. Dadurch ist auf der Menge der 1-Kozykeln eine Äquivalenzrelation definiert. Die Menge der Klassen kohomolog 1-Kozykeln heißt erste Amitsursche Kohomologiemenge und wird mit $H^1(S/R, F)$ bezeichnet (vgl. [29] S. 63). Sie ist durch die Klasse des neutralen Elementes von $F(S \otimes S)$ punktiert.

Bekannter ist die Amitsursche Kohomologie von Ab-wertigen Funktoren F . Die Struktur von $F(S \otimes S)$ induziert dabei eine abelsche Gruppenstruktur auf $H^1(S/R, F)$.

Die gruppenwertigen Funktoren auf R-Alg bilden eine Kategorie $\underline{Funkt}(\underline{R\text{-Alg}}, \underline{Grp})$. (Die mengentheoretischen Schwierigkeiten dieser Bildung lassen sich bekanntlich durch einen geeigneten Aufbau der Kategorientheorie be-

heben.)

$H^1(-/R, -) : \underline{R-Alg} \times \underline{Funkt}(\underline{R-Alg}, \underline{Grp}) \longrightarrow \underline{Me}^*$ ist ein Funktor. Er operiert auf den Morphismen in naheliegender Weise.

Betrachten wir die Beispiele (2.2.) und (2.3.), so wird klar, daß noch gewisse gruppenwertige Funktoren einzuführen sind.

(2.13.) Definition. R , $\underline{A}$ und $(A, \mathcal{A})$ seien wie in (2.5.). $\underline{Aut}(A, \mathcal{A}) : \underline{R-Alg} \longrightarrow \underline{Grp}$ ordnet einer R -Algebra T die Gruppe der $\underline{A}_T$ -Automorphismen von $(A_T, \mathcal{A}_T)$ zu, und für $d : S \longrightarrow T$ sei $\underline{Aut}(A, \mathcal{A})(d)$ der Gruppenhomomorphismus

$$\underline{A}_S\text{-aut}(A_S, \mathcal{A}_S) \ni \sigma \longmapsto d^*(\sigma) \in \underline{A}_T\text{-aut}(A_T, \mathcal{A}_T).$$

Daß diese Vorschrift einen Funktor definiert, folgt unmittelbar aus den Gleichungen $(d \circ d')^* = d^* \circ d'^*$, $\text{id}^* = \text{Id}$ (vgl. 2.5.3.).

Betrachten wir diesen Funktor nun im Beispiel der verzerrten $\underline{G}$ -Formen der trivialen G -Galoiserweiterung.

(2.14.) Proposition. Der Endomorphismenring des $R[G]$ -Moduls E_R^G ist zum Gruppenring $R[G]$ isomorph. Der Isomorphismus ist durch folgende Vorschrift bestimmt

$$\Gamma : \underline{R[G]\text{-Mod}}(E_R^G, E_R^G) \longrightarrow R[G]$$

$$f \longmapsto \sum_g r_g g^{-1} u_g, \text{ falls } f(v_e) = \sum_g r_g v_g.$$

Die Gruppe $G_R\text{-aut}(E_R^G) = \text{Gal}(R, G)\text{-aut}(E_R^G)$ wird durch Γ isomorph auf $V(R[G])$ abgebildet. Dabei ist $V(R[G])$ folgende Untergruppe der Einheitengruppe $U(R[G])$

$$V(R[G]) := \left\{ \sum_g r_g u_g \in R[G] \mid r_g r_h = \delta_{g,h} r_g \text{ und } \sum_g r_g = 1 \right\}.$$

Beweis. Die Auswertung $R[G]\text{-Mod}(R[G], R[G]) \longrightarrow R[G]$, $f \longmapsto f(1)$ ist bekanntlich ein Antiisomorphismus von Ringen. Verknüpft man sie mit der Antipode des Gruppenringes und berücksichtigt den Isomorphismus α aus (2.9.), so erhält man Γ . Die Einheiten von $R[G]$ entsprechen unter Γ den Automorphismen des $R[G]$ -Moduls E_R^G .

Sei $f : E_R^G \longrightarrow E_R^G$ ein $R[G]$ -Modulautomorphismus, und es sei $f(v_e) = \sum_g r_g v_g$.

f ist genau dann multiplikativ, wenn für alle $g, h \in G$ gilt $f(v_g v_h) = f(v_g) f(v_h)$. Nun ist $f(v_g) f(v_h) = (g f(v_e)) (h f(v_e)) = (\sum_{g'} r_{g'} v_{gg'}) (\sum_{h'} r_{h'} v_{hh'}) = \sum_{g'} r_{g'} r_h^{-1} v_{gg'}$. Daraus erkennt man, daß f genau dann multiplikativ ist, wenn für alle $g, h \in G$

$$r_g r_h = \begin{cases} r_g, & \text{falls } g = h \\ 0, & \text{sonst} \end{cases}.$$

Unitär ist f genau dann, wenn $\sum_g r_g = 1$ ist, denn

$$\begin{aligned} 1 &= f(1) = f\left(\sum_g v_g\right) = \sum_g \left(\sum_{g'} r_{g'}^{-1} v_{g'g}\right) = \\ &= \sum_{g'} \left(\sum_g r_{g'}^{-1} v_{g'g}\right) v_{g'} = \sum_{g'} \left(\sum_h r_h\right) v_{g'}. \end{aligned}$$

(2.15.) Bezeichnung. $V(-[G]) : \underline{R}\text{-Alg} \longrightarrow \underline{\text{Grp}}$ sei der Funktor, welcher eine R -Algebra S auf $V(S[G])$ schickt und $q : S \longrightarrow T$ auf $V(S[G]) \ni \sum_g s_g u_g \longmapsto \sum_g q(s_g) u_g \in V(T[G])$ abbildet.

§ 2 Der Hauptsatz der Theorie der verzerrten Formen

Wir formulieren das gesamte Konzept des Übergangs von den verzerrten Formen zur Amitsurschen Kohomologie in einem einzigen Satz. Den Beweis führen wir jedoch in mehreren Schritten.

(2.16.) Theorem. Seien $\underline{A}$ eine zulässige Struktur, $R \hookrightarrow S$ eine treuflache Erweiterung und $(A, \mathcal{A}) \in \underline{A}_R$.

Die Menge der verzerrten Formen von $(A, \mathcal{A})$ bezüglich $R \hookrightarrow S$ entspricht bijektiv der Menge $H^1(S/R, \underline{\text{Aut}}(A, \mathcal{A}))$.

Die Bijektion ist folgendermaßen bestimmt

- i.) Einer verzerrten Form $[B, \mathfrak{B}]$ mit einem $\underline{A}_S$ -Isomorphismus $\beta : (B_S, \mathfrak{B}_S) \xrightarrow{\sim} (A_S, \mathcal{A}_S)$ wird die Klasse des 1-Kozykels

$$A_S \otimes S \xrightarrow{d_1^*(\beta)^{-1}} B_S \otimes S \xrightarrow{d_2^*(\beta)} A_S \otimes S$$

zugeordnet.

- ii.) Für einen 1-Kozykel k sei B der Differenzkern des Paares von R -Modulhomomorphismen

$$A_S \xrightarrow[k(A \otimes d_1)]{A \otimes d_2} A_S \otimes S.$$

Die Skalarmultiplikation von A_S induziert einen Isomorphismus $\lambda : B_S \xrightarrow{\sim} A_S$, und es gibt auf B genau eine $\underline{A}$ -Struktur $\mathfrak{B}$, so daß $\lambda : (B_S, \mathfrak{B}_S) \longrightarrow (A_S, \mathcal{A}_S)$ ein $\underline{A}$ -Isomorphismus ist. Der Klasse $[k]$ wird die verzerrte Form $[B, \mathfrak{B}]$ zugeordnet.

Die beschriebene Bijektion ist ein funktorieller Isomorphismus zwischen den Funktoren $V_{\underline{A}}^-(A, \mathcal{A})$ und $H^1(-/R, \underline{\text{Aut}}(A, \mathcal{A}))$.

Als erste Anwendung betrachten wir die Aussage des Theorems im Fall von G -Galoiserweiterungen.

(2.17.) Folgerung. Ist G eine endliche Gruppe und $R \hookrightarrow S$ eine treuflache Erweiterung, so gibt es eine Bijektion punktierter Mengen $\text{Gal}(S/R, G) \xrightarrow{\sim} H^1(S/R, V(-[G]))$. Sie ist funktoriell in S .

Beweis. Da $\underline{G}$ eine zulässige Struktur ist, sind die punktierten Mengen $V_{\underline{G}}^S(E_R^G) \xrightarrow{\sim} H^1(S/R, \underline{\text{Aut}} E_R^G)$ funktoriell isomorph (2.16.). Die verzerrten Formen von E_R^G bezüglich S entsprechen aber gerade $\text{Gal}(S/R, G)$ (2.10.), und in (2.14.) wurde gezeigt, daß $\underline{G}_S\text{-aut}(E_S^G) \xrightarrow{\sim} V(S[G])$ isomorphe Gruppen sind. Man prüft schnell nach, daß der in (2.14.) angegebene Isomorphismus Γ in S funktoriell ist.

Den Beweis von (2.16.) führen wir in mehreren Schritten.

(2.16.1.) Die in i.) definierte Zuordnung

$V_{\underline{A}}^S(A, \mathcal{A}) \rightarrow H^1(S/R, \underline{\text{Aut}}(A, \mathcal{A}))$ ist wohldefiniert.

Beweis von (2.16.1.). Sei $[B, \mathcal{B}]$ eine verzerrte Form von $(A, \mathcal{A})$ bezüglich S . Da im Amitsurschen Komplex die Relationen $d_1 \eta_S = \eta_{S \otimes S} = d_2 \eta_S$ gelten, kann man für einen $\underline{A}_S$ -Isomorphismus

$\beta : (B_S, \mathcal{B}_S) \xrightarrow{\sim} (A_S, \mathcal{A}_S)$ die $\underline{A}_{S \otimes S}$ -Isomorphismen $d_1^*(\beta)^{-1}$ und $d_2^*(\beta)$ verknüpfen.

$k := d_2^*(\beta) d_1^*(\beta)^{-1}$ ist ein $\underline{A}_{S \otimes S}$ -Automorphismus von $(A_{S \otimes S}, \mathcal{A}_{S \otimes S})$.

Nun wollen wir zeigen $k_2 = k_3 k_1$. Die Relationen $d_3 d_1 = d_1 d_2$, $d_3 d_2 = d_2 d_2$, $d_2 d_1 = d_1 d_1$ der Morphismen aus Amitsurs Komplex sind das entscheidende Hilfsmittel. Mit ihnen sieht man

$$\begin{aligned} k_3 k_1 &= d_3^*(k) d_1^*(k) \\ &= (d_3 d_2)^*(\beta) (d_3 d_1)^*(\beta)^{-1} (d_1 d_2)^*(\beta) (d_1 d_1)^*(\beta)^{-1} \\ &= (d_2 d_2)^*(\beta) (d_1 d_2)^*(\beta)^{-1} (d_1 d_2)^*(\beta) (d_2 d_1)^*(\beta)^{-1} \\ &= d_2^*(k) = k_2. \end{aligned}$$

Es bleibt zu zeigen, daß die Klasse $[k]$ unabhängig vom gewählten Isomorphismus β ist. Sei β' ein weiterer $\underline{A}_S$ -Isomorphismus, k' sei der zugehörige

1-Kozykel. Dann sind k und k' kohomolog, denn für $l_1 := \beta' \beta^{-1} \in \underline{A}_S\text{-Aut}(A_S, \mathcal{A}_S)$ gilt $l_2 k l_1^{-1} =$
 $= (d_2^*(\beta') d_2^*(\beta)^{-1})(d_2^*(\beta) d_1^*(\beta)^{-1})(d_1^*(\beta') d_1^*(\beta)^{-1})^{-1}$
 $= d_2^*(\beta') d_1^*(\beta')^{-1} = k'.$

(2.16.2.). Für den in ii.) beschriebenen R -Modul $B \hookrightarrow A_S$ induziert die Skalarmultiplikation einen Isomorphismus $\lambda: B_S \xrightarrow{\sim} A_S$ von S -Moduln.

Beweis von (2.16.2.). Sei $k \in \underline{A}_{S \otimes S}\text{-Aut}(A_{S \otimes S}, \mathcal{A}_{S \otimes S})$ ein 1-Kozykel. In der Terminologie der Abstiegstheorie ist k eine Abstiegsmöglichkeit des S -Moduls A_S entlang der treuflachen Erweiterung $R \hookrightarrow S$ (vgl. [29] S. 35). Die Technik des treuflachen Abstiegs vereinfacht sich in unserer Situation, da die üblicherweise betrachteten $S \otimes S$ -Moduln $S \otimes A_S \simeq d_1^*(A_S)$ und $A_S \otimes S \simeq d_2^*(A_S)$ beide kanonisch isomorph zu $A_{S \otimes S} \simeq (d_2 d_1)^*(A) \simeq (d_1 d_1)^*(A)$ sind.

Wir wollen den Beweis von Knus und Ojanguren ([29] Chap.2, §3) mit unseren Bezeichnungen nachvollziehen.

Wir definieren den R -Modul B als den Differenzkern

$$0 \longrightarrow B \longrightarrow A \otimes S \xrightarrow[k(A \otimes d_1)]{A \otimes d_2} A \otimes S \otimes S.$$

Nun betrachten wir das Diagramm von S -Modulhomomorphismen

$$\begin{array}{ccccccc}
 0 \longrightarrow S \otimes B & \longrightarrow & S \otimes A \otimes S & \xrightarrow[\quad (S \otimes k)(S \otimes A \otimes d_1) \quad]{S \otimes A \otimes d_2} & S \otimes A \otimes S \otimes S \\
 \downarrow \lambda & & \downarrow \tau \otimes S & & \downarrow \tau \otimes S \\
 & & A \otimes S \otimes S & & A \otimes S \otimes S \otimes S \\
 & & \downarrow \int k & & \downarrow \text{kan} \\
 & & & & d_3^*(A \otimes S \otimes S) \\
 & & & & \downarrow k_3 \\
 & & & & d_3^*(A \otimes S \otimes S) \\
 & & & & \downarrow \text{kan} \\
 0 \longrightarrow A \otimes S & \longrightarrow & A \otimes S \otimes S & \xrightarrow[\quad A \otimes S \otimes d_1 \quad]{A \otimes S \otimes d_2} & A \otimes S \otimes S \otimes S
 \end{array}$$

Da S treuflach ist, sind die obere und die untere Zeile exakt (vgl. [29] Chap. 2 Prop. 2.1.). Das rechte Viereck kommutiert sowohl mit den oberen als auch mit den unteren Pfeilen:

$$\begin{aligned}
 & k_3 (\tau \otimes S) (S \otimes A \otimes d_2) (s \otimes a \otimes s') \\
 &= k_3 (a \otimes s \otimes s' \otimes 1) = k (a \otimes s \otimes s') \otimes 1 = \\
 &= (A \otimes S \otimes d_2) k (\tau \otimes S) (s \otimes a \otimes s')
 \end{aligned}$$

$$\begin{aligned}
 & k_3 (\tau \otimes S) (S \otimes k) (S \otimes A \otimes d_1) (s \otimes a \otimes s') \\
 &= k_3 (\tau \otimes S) (s \otimes k (a \otimes 1 \otimes s')) = k_3 k_1 (a \otimes s \otimes 1 \otimes s') \\
 &= k_2 (a \otimes s \otimes 1 \otimes s') = (A \otimes S \otimes d_1) k (a \otimes s \otimes s') .
 \end{aligned}$$

Da die senkrechten Pfeile bijektiv sind, induziert k einen S -Modulisomorphismus $\lambda : B_S \longrightarrow A_S$.

Für $1 \otimes b \in S \otimes B$ gilt

$$\begin{aligned} (A \otimes S \otimes \eta) \lambda (1 \otimes b) &= k(\tau \otimes S) (1 \otimes b) \\ &= k(A \otimes d_1) (b) = (A \otimes d_2) (b) = (A \otimes S \otimes \eta) (b). \end{aligned}$$

Deshalb ist $\lambda (1 \otimes b) = b$ und $\lambda (s \otimes b) = s \cdot b$.

λ wird also von der Skalarmultiplikation auf A_S induziert.

Wir wollen noch zeigen, daß B genau eine $\underline{A}$ -Struktur $\mathcal{B}$ trägt, für welche λ ein $\underline{A}_S$ -Isomorphismus ist. Sei $\varphi : x \longrightarrow y$ aus $\underline{A}$. Falls eine solche Struktur existiert, so kommutiert das Diagramm

$$\begin{array}{ccc} F_x^R(B) \otimes S & \xrightarrow{\mathcal{B}(\varphi) \otimes S} & F_y^R(B) \otimes S \\ \downarrow \phi_x^{\eta} \wr & & \downarrow \wr \phi_y^{\eta} \\ F_x^S(B_S) & \xrightarrow{\mathcal{B}_S(\varphi)} & F_y^S(B_S) \\ \downarrow \wr & & \downarrow \wr \\ F_x^S(\lambda) & & F_y^S(\lambda) \\ \downarrow & & \downarrow \\ F_x^S(A_S) & \xrightarrow{\mathcal{A}_S(\varphi)} & F_y^S(A_S) \end{array} \quad (2.16.2.*)$$

$\mathcal{B}(\varphi) \otimes S$ und damit auch $\mathcal{B}(\varphi)$ sind also eindeutig, falls sie existieren.

Um die Existenz einer $\underline{A}$ -Struktur auf B zeigen zu können, benötigen wir noch folgende Aussage:

(2.16.3.) Zwischen dem 1-Kozykel k und dem S -Modulisomorphismus λ besteht die Relation $k d_1^*(\lambda) = d_2^*(\lambda)$.

Beweis von (2.16.3.). Dazu betrachten wir das Diagramm von $S \otimes S$ -Modulhomomorphismen

$$\begin{array}{ccccccc}
 B \otimes S \otimes S & \xrightarrow{\sim} & d_2^*(B_S) & \xrightarrow{\sim} & B_S \otimes S & \xrightarrow{\sim} & d_1^*(B_S) \xrightarrow{\sim} S \otimes B \otimes S \\
 \lambda \otimes S \downarrow & & \downarrow d_2^*(\lambda) & & & & \downarrow S \otimes \lambda \\
 A \otimes S \otimes S & \xrightarrow{\sim} & d_2^*(A_S) & & d_1^*(\lambda) & & \\
 \uparrow k & & & & \downarrow & & \downarrow \\
 A \otimes S \otimes S & \xrightarrow{\sim} & d_2^*(A_S) \xrightarrow{\sim} A_S \otimes S & \xrightarrow{\sim} & d_1^*(A_S) \xrightarrow{\sim} S \otimes A \otimes S.
 \end{array}$$

Alle horizontalen Pfeile sind kanonische Isomorphismen von $S \otimes S$ -Moduln. Es zeigt sich, daß ihre Komposition mit $\tau \otimes S : B \otimes S \otimes S \xrightarrow{\sim} S \otimes B \otimes S$ übereinstimmt. Wir wollen also zeigen

$\lambda \otimes S = k(\tau \otimes S)(S \otimes \lambda)(\tau \otimes S)$. Seien dazu $s, s' \in S$, und $b \in B \hookrightarrow A \otimes S$ habe in $A \otimes S$ die Form $b = \sum a_i \otimes s_i$.

$$\begin{aligned}
 & k(\tau \otimes S)(S \otimes \lambda)(\tau \otimes S)(b \otimes s \otimes s') \\
 &= k(\tau \otimes S)(s \otimes (\sum a_i \otimes s_i)s') \\
 &= k(\sum a_i \otimes s \otimes s_i s') = k(s \otimes s'(\sum a_i \otimes 1 \otimes s_i)) \\
 &= (s \otimes s') k(\sum a_i \otimes 1 \otimes s_i) = (s \otimes s')(\sum a_i \otimes s_i \otimes 1) \\
 &= \sum a_i \otimes s_i s \otimes s' = (\sum a_i \otimes s_i) s \otimes s' \\
 &= \lambda \otimes S(b \otimes s \otimes s').
 \end{aligned}$$

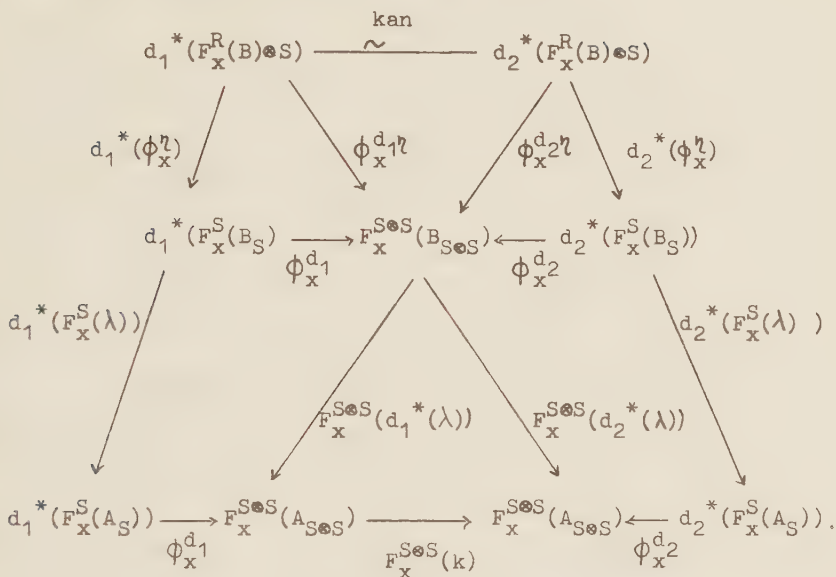
(2.16.4.) Seien k, B, λ wie in (2.16.ii.). Für jeden Morphismus $\varphi : x \rightarrow y$ aus $\underline{A}$ gibt es genau einen R -Modulhomomorphismus $\mathcal{B}(\varphi) : F_x^R(B) \rightarrow F_y^R(B)$, so daß das Diagramm (2.16.2.*) kommutiert.

Beweis von (2.16.4.). Sei $u : F_x^R(B) \otimes S \rightarrow F_y^R(B) \otimes S$ der S -Modulhomomorphismus, welcher (2.16.2.*) kommutativ macht. Der treuflache Abstieg von Homomorphismen zeigt, daß es genügt $d_1^*(u) = d_2^*(u)$ nachzuweisen (vgl. [29] Chap.2. Prop. 2.5.).

Dasselbe Problem tritt beim Abstieg von Algebren auf, und der Beweis von Knus und Ojanguren ([29] S.39) dient uns als Vorbild. Da bei uns neben kanonischen Isomorphismen auch noch die funktoriellen Isomorphismen ϕ auftreten, können wir nicht so unbeschwert identifizieren, wie es im Algebrenfall möglich ist. Entlang der kanonischen Isomorphismen identifizieren wir aber auch, so daß das Diagramm (2.16.3.) folgende Gestalt annimmt

$$\begin{array}{ccc}
 & B_S \otimes S & \\
 d_1^*(\lambda) \swarrow & & \searrow d_2^*(\lambda) \\
 A_S \otimes S & \xrightarrow{k} & A_S \otimes S
 \end{array}$$

Nun betrachten wir folgendes Diagramm



Das untere Dreieck kommutiert, da $k d_1^*(\lambda) = d_2^*(\lambda)$ ist (vgl. 2.16.3.), das obere Dreieck wegen $d_1 \eta = d_2 \eta$. Die seitlichen Drei- und Vierecke kommutieren auf Grund der Eigenschaften der ϕ (vgl. 2.5.1.).

Ein analoges Diagramm erhalten wir, wenn wir x durch y ersetzen. Den Übergang zwischen diesen beiden Diagrammen ermöglichen von φ bzw. u induzierte Morphismen, welche ein weiteres kommutatives Diagramm ergeben.

$$\begin{array}{ccc}
 d_1^*(F_x^R(B) \otimes S) & \xrightarrow{d_1^*(u)} & d_1^*(F_y^R(B) \otimes S) \\
 \downarrow d_1^*(F_x^S(\lambda) \phi_x^\eta) & & \downarrow d_1^*(F_y^S(\lambda) \phi_y^\eta) \\
 d_1^*(F_x^S(A_S)) & \xrightarrow{d_1^*(\mathcal{A}_S(\varphi))} & d_1^*(F_y^S(A_S)) \\
 \downarrow \phi_x^{d_1} & & \downarrow \phi_y^{d_1} \\
 F_x^{S \otimes S}(A_{S \otimes S}) & \xrightarrow{\mathcal{A}_{S \otimes S}(\varphi)} & F_y^{S \otimes S}(A_{S \otimes S}) \\
 \downarrow F_x^{S \otimes S}(k) & & \downarrow F_y^{S \otimes S}(k) \\
 F_x^{S \otimes S}(A_{S \otimes S}) & \xrightarrow{\mathcal{A}_{S \otimes S}(\varphi)} & F_y^{S \otimes S}(A_{S \otimes S}) \\
 \downarrow \phi_x^{d_2} & & \downarrow \phi_y^{d_2} \\
 d_2^*(F_x^S(A_S)) & \xrightarrow{d_2^*(\mathcal{A}_S(\varphi))} & d_2^*(F_y^S(A_S)) \\
 \uparrow d_2^*(F_x^S(\lambda) \phi_x^\eta) & & \uparrow d_2^*(F_y^S(\lambda) \phi_y^\eta) \\
 d_2^*(F_x^R(B) \otimes S) & \xrightarrow{d_2^*(u)} & d_2^*(F_y^R(B) \otimes S)
 \end{array}$$

Die äußeren beiden Vierecke kommutieren, da sie durch Funktoren aus (2.16.2*) entstehen. Das mittlere Viereck kommutiert, da k ein $\underline{A}_{S \otimes S}$ -Morphismus ist. Bei den restlichen Vierecken geht ein, daß die ϕ funktoriell sind.

Eine Diagrammjagd zeigt nun

$$\begin{aligned}
 & \phi_y^{d_2} d_2^*(F_y^S(\lambda) \phi_y^\eta) d_2^*(u) \text{ kan} \\
 & = \mathcal{A}_{S \otimes S}(\varphi) \phi_x^{d_2} d_2^*(F_x^S(\lambda)) d_2^*(\phi_x^\eta) \text{ kan} \\
 & = \mathcal{A}_{S \otimes S}(\varphi) F_x^{S \otimes S}(d_2^*(\lambda)) \phi_x^{d_1 \eta}
 \end{aligned}$$

$$\begin{aligned}
 &= \mathcal{A}_{S \otimes S}(\varphi) \quad F_x^{S \otimes S}(k) \quad F_x^{S \otimes S}(d_1^*(\lambda)) \quad \phi_x^{d_1 \eta} \\
 &= F_y^{S \otimes S}(k) \quad \mathcal{A}_{S \otimes S}(\varphi) \quad \phi_x^{d_1} \quad d_1^*(F_x^S(\lambda) \phi_x^\eta) \\
 &= F_y^{S \otimes S}(k) \quad \phi_y^{d_1} \quad d_1^*(F_y^S(\lambda) \phi_y^\eta) \quad d_1^*(u) \\
 &= F_y^{S \otimes S}(k) \quad F_y^{S \otimes S}(d_1^*(\lambda)) \quad \phi_y^{d_1 \eta} \quad d_1^*(u) \\
 &= \phi_y^{d_2} \quad d_2^*(F_y^S(\lambda)) \quad d_2^*(\phi_y^\eta) \quad \text{kan} \quad d_1^*(u) .
 \end{aligned}$$

Also ist auch $d_2^*(u) \text{ kan} = \text{kan} \, d_1^*(u)$.

(2.16.5.). Die in ii.) definierte Zuordnung
 $H^1(S/R, \underline{\text{Aut}}(A, \mathcal{A})) \longrightarrow V_{\underline{A}}^S(A, \mathcal{A})$ ist wohldefiniert.

Beweis von (2.16.5.). Seien k, k' Kohomologe

1-Kozykeln, und für $l \in \underline{A}_S\text{-aut}(A_S, \mathcal{A}_S)$ sei

$$k' = l_2 k l_1^{-1} . \quad \text{Aus } k = d_2^*(\lambda) d_1^*(\lambda)^{-1},$$

$$k' = d_2^*(\lambda') d_1^*(\lambda')^{-1} \quad \text{schließen wir: } k' l_1 = l_2 k$$

$$\implies d_2^*(\lambda') d_1^*(\lambda')^{-1} d_1^*(l) = d_2^*(l) d_2^*(\lambda) d_1^*(\lambda)^{-1}$$

$$\implies d_1^*(\lambda'^{-1} l \lambda) = d_2^*(\lambda'^{-1} l \lambda) . \quad \text{Treuflacher}$$

Abstieg von Homomorphismen zeigt nun, daß es einen

Homomorphismus $f : B \longrightarrow B'$ von R -Moduln gibt, mit

$$f_S = (\lambda')^{-1} l \lambda . \quad \text{Da } f_S \text{ bijektiv ist und ein}$$

$\underline{A}_S$ -Morphismus, ist bereits f bijektiv und ein

$\underline{A}_R$ -Morphismus.

Beweis von Satz (2.16.). Wir haben bisher gesehen,

daß beide Zuordnungen wohldefiniert sind. Dabei

führten wir einige typische Überlegungen sehr aus-

föhrlich vor, so daß wir uns nun kurz fassen können.

Ist k ein 1-Kozykel, $(B, \mathfrak{B})$ das in ii.) beschriebene $\underline{A}_R$ -Objekt, so ordnet i.) der verzerrten Form $[B, \mathfrak{B}]$ den 1-Kozykel $d_2^*(\lambda) d_1^*(\lambda)^{-1} = k$ zu (vgl. 2.16.3.). Sei nun umgekehrt eine verzerrte Form $[B, \mathfrak{B}]$ gegeben. $k' := d_2^*(\beta) d_1^*(\beta)^{-1}$ sei der gemäß i.) konstruierte 1-Kozykel. Darauf wenden wir ii.) an und nennen das erhaltene $\underline{A}_R$ -Objekt $(B', \mathfrak{B}')$ und die Skalarmultiplikation

$\lambda : B'_S \xrightarrow{\sim} A_S$. Man überlegt sich, daß für $B \otimes S \xrightarrow{\beta} A \otimes S \xrightarrow{\lambda^{-1}} B' \otimes S$ $d_1^*(\lambda^{-1}\beta) = d_2^*(\lambda^{-1}\beta)$ ist. Nach dem Satz über den treuflachen Abstieg von Homomorphismen ([29] Chap.2. Prop. 2.5.) gibt es einen Homomorphismus von R -Moduln $f : B \rightarrow B'$, so daß $f_S = \lambda^{-1}\beta$ ist. f_S ist bijektiv und ein $\underline{A}_S$ -Morphismus. Da S treuflach ist, ist bereits f bijektiv und ein $\underline{A}_R$ -Morphismus. Also sind die beiden Zuordnungen invers zueinander.

Wir verzichten darauf, zu verifizieren, daß die Zuordnungen funktoriell in S sind und zeigen nur noch, daß die ausgezeichneten Punkte ineinander übergehen. Der Kozykel $\text{id} \in \underline{A}_{S \otimes S}\text{-aut}(A_{S \otimes S}, \mathcal{A}_{S \otimes S})$ ist ein Repräsentant der ausgezeichneten Klasse. Ihm wird gemäß ii.) der Differenzkern von

$$A \otimes S \xrightleftharpoons[A \otimes d_1]{A \otimes d_2} A \otimes S \otimes S$$

zugeordnet. Da S treuflach ist, ist dies $A \xrightarrow{A \otimes \eta} A \otimes S$. Die Struktur $\mathcal{A}$ erfüllt die Bedingungen von ii.). Deshalb wird $[\text{id}]$ die verzerrte Form $[A, \mathcal{A}]$ zugeordnet.

§ 3 Beschreibung der Ecken des Invarianten-Diagrammes mit Amitsurscher Kohomologie

Nachdem wir die Theorie der verzerrten Formen so weit entwickelt haben, wie wir sie benötigen, können wir uns wieder dem zuwenden, was uns eigentlich interessiert. Zuerst ergänzen wir unsere Ergebnisse über $\text{Gal}({}^S\text{R}/\text{R}, \text{G})$. Der Spezialfall abelscher Galois-erweiterungen, insbesondere quadratischer Erweiterungen, soll noch betrachtet werden.

Ist die endliche Gruppe G abelsch, so sind die Gruppenringe $S[G]$, $S \in \underline{\text{R-Alg}}$ kommutativ. Der Funktor $V(-[G])$ nimmt deshalb seine Werte in den abelschen Gruppen an. $H^1({}^S\text{R}/\text{R}, V(-[G]))$ trägt die Struktur einer abelschen Gruppe (2.12.), und $\text{Gal}({}^S\text{R}/\text{R}, \text{G})$ ist als Kern des Homomorphismus $\text{Gal}(\text{R}, \text{G}) \longrightarrow \text{Gal}(\text{S}, \text{G})$ ebenfalls eine abelsche Gruppe.

(2.18.) Satz. Ist G eine endliche abelsche Gruppe und $\text{R} \hookrightarrow \text{S}$ eine treuflache Erweiterung, so ist die Bijektion aus (2.17.) ein Isomorphismus abelscher Gruppen $\text{Gal}({}^S\text{R}/\text{R}, \text{G}) \simeq H^1({}^S\text{R}/\text{R}, V(-[G]))$.

Beweis. Seien k, k' 1-Kozykeln in $\underline{G}_S \otimes_S \text{-aut}(\underline{E}_{S \otimes S}^G)$.

A, A' seien die dazu gemäß (2.16.ii) konstruierten G -Galoiserweiterungen von R , und $\lambda: A \otimes S \xrightarrow{\sim} \underline{E}_S^G$, $\lambda': A' \otimes S \xrightarrow{\sim} \underline{E}_S^G$ seien die jeweiligen Skalarmultiplikationen.

Wir wollen zeigen, daß sich die Klassen $[A][A']$ und $[k][k']$ entsprechen. Dazu konstruieren wir zunächst gemäß (2.16.i) den Kozykel zur verzerrten Form $[A][A'] = [(A \otimes A')^\Delta]$ (vgl. 1.39.).

Betrachten wir folgendes Diagramm

$$(2.18.1.) \quad \begin{array}{ccccc} A \otimes A' \otimes S & \xrightarrow[\sim]{\text{kan}} & A_S \otimes_S A'_S & \xrightarrow[\sim]{\lambda \otimes \lambda'} & E_S^G \otimes_S E_S^G \\ \uparrow \text{inkl} & & & & \uparrow \\ (A \otimes A')^\Delta \otimes S & \xrightarrow[\sim]{\sigma} & & & (E_S^G \otimes_S E_S^G)^\Delta \\ & & & & \uparrow \pi \\ & & & & E_S^G \end{array}$$

Die obere Zeile ist ein Isomorphismus von $(G \times G)$ -Galoiserweiterungen. Sie induziert daher einen Isomorphismus von G -Galoiserweiterungen auf den Fixringen bezüglich Δ . Ist π ein $\text{Gal}(S, G)$ -Isomorphismus — nach (1.39.) existiert ein solcher —, so ergibt sich daraus ein $\text{Gal}(S, G)$ -Isomorphismus σ .

In $k'' := d_2^*(\sigma) \cdot d_1^*(\sigma)^{-1}$ haben wir damit einen 1-Kozykel zu $(A \otimes A')^\Delta$ gefunden. Wir wollen nun nicht nur $[k''] = [k][k']$ zeigen, sondern sogar $k'' = kk'$ bzw. $\Gamma(k'') = \Gamma(k)\Gamma(k')$, was nach (2.14.) dasselbe ist.

Um π angeben zu können, überlegen wir:

$$\begin{aligned} \sum_{g,h} s_{g,h} \cdot v_g \otimes v_h &\in (E_S^G \otimes_S E_S^G)^\Delta \\ \iff \forall g' \in G : \sum_{g,h} s_{g,h} \cdot v_g \otimes v_h &= \sum_{g,h} s_{g,h} \cdot v_{g'g} \otimes v_{g'^{-1}h} \end{aligned}$$

$\Leftrightarrow \forall g, h \in G : s_{g,h} = s_{hg,e}$. Die Elemente von

$(E_S^G \otimes_S E_S^G)^\Delta$ sind also von der Form

$$\sum_h s_h \left(\sum_g v_g \otimes v_{hg}^{-1} \right) = \left(\sum_h s_h u_h \right) \left(\sum_g v_g \otimes v_g^{-1} \right).$$

Als $S[G]$ -Modul wird $(E_S^G \otimes_S E_S^G)^\Delta$ vom Element

$\sum_g v_g \otimes v_g^{-1}$ frei erzeugt. Der $S[G]$ -Modulisomorphismus

$$E_S^G \xrightarrow{\sim} (E_S^G \otimes_S E_S^G)^\Delta, \text{ der durch } v_e \mapsto \sum_g v_g \otimes v_g^{-1}$$

definiert wird, ist auch mit den Algebrenstrukturen verträglich. Dies ist also unser π .

Im folgenden unterscheiden wir die Basiselemente von

$E_R^G, E_S^G, E_{S \otimes S}^G$, indem wir den Ring als zusätzlichen Index anfügen. Außerdem vereinbaren wir folgende Bezeichnungen:

Es seien $\sum_i a_i \otimes s_i \in A \otimes S$, $\sum_j a'_j \otimes s'_j \in A' \otimes S$ mit

$$\sum_i a_i \otimes s_i = \sum_j a'_j \otimes s'_j = v_e^S, \text{ und } a_i = \sum_g v_g^R \otimes a_{ig},$$

$a'_j = \sum_g v_g^R \otimes a'_{jg}$ seien die jeweiligen Basisdarstellungen in $E_R^G \otimes S$.

$$\text{Damit ist } k(v_e^{S \otimes S}) = d_2^*(\lambda) d_1^*(\lambda)^{-1} (v_e^{S \otimes S})$$

$$= (\lambda \otimes S) (\tau \otimes S) (S \otimes \lambda^{-1}) (1 \otimes v_e^R \otimes 1)$$

$$= (\lambda \otimes S) \left(\sum_i a_i \otimes 1 \otimes s_i \right) = \sum_i a_i \otimes s_i =$$

$$= \sum_i \sum_g v_g^R \otimes a_{ig} \otimes s_i = \sum_g \left(\sum_i a_{ig} \otimes s_i \right) v_g^{S \otimes S}.$$

Nach (2.14.) ist deshalb $\Gamma(k) = \sum_g \left(\sum_i a_{ig}^{-1} \otimes s_i \right) u_g$.

Analog sind $k'(v_e^{S \otimes S}) = \sum_g \left(\sum_j a'_{jg} \otimes s'_j \right) v_g^{S \otimes S}$ und

$$\Gamma(k') = \sum_g \left(\sum_j a'_{jg}^{-1} \otimes s'_j \right) u_g.$$

Um $\Gamma(k'')$ zu bestimmen, verwenden wir folgenden Hilfsatz.

(2.18.2). Für $c_{ij} := \sum_g g(a_i) g^{-1}(a'_j)$

$\in A \otimes A'$ gelten :

a.) $c_{ij} \in (A \otimes A')^\Delta$

b.) $\sigma \left(\sum_{i,j} c_{ij} \otimes s_i \cdot s'_j \right) = v_e^S$

c.) $\sigma(c_{ij} \otimes 1) = \sum_g \left(\sum_h a_{ih} a'_{j(h^{-1}g)} \right) v_g^S$

Beweis von (2.18.2). a.) Klar.

b.) $\pi^{-1}(\lambda \otimes \lambda') \text{ kan } \left(\sum c_{ij} \otimes s_i \cdot s'_j \right)$

$$= \pi^{-1}(\lambda \otimes \lambda') \left(\sum_g \left(\sum_i g(a_i) \otimes s_i \right) \otimes_S \left(\sum_j g^{-1}(a'_j) \otimes s'_j \right) \right)$$

$$= \pi^{-1} \left(\sum_g g \lambda \left(\sum_i a_i \otimes s_i \right) \otimes_S g^{-1} \lambda' \left(\sum_j a'_j \otimes s'_j \right) \right)$$

$$= \pi^{-1} \left(\sum_g v_g^S \otimes_S v_{g^{-1}}^S \right) = v_e^S.$$

c.) $\sigma(c_{ij} \otimes 1) = \pi^{-1}(\lambda \otimes \lambda') \text{ kan } \left(\sum_g g(a_i) \otimes g^{-1}(a'_j) \otimes 1 \right)$

$$= \pi^{-1} \left(\sum_g g \left(\sum_h v_h^R \otimes a_{ih} \right) \otimes_S g^{-1} \left(\sum_{h'} v_{h'}^R \otimes a'_{jh'} \right) \right)$$

$$= \pi^{-1} \left(\sum_g \sum_h \sum_{h'} a_{ih} a'_{jh'} (v_{gh}^S \otimes_S v_{g^{-1}h'}^S) \right)$$

$$\begin{aligned}
 &= \mathfrak{P}^{-1} \left(\sum_g \sum_n \sum_{g'} a_{ih} a'_{j(h^{-1}g)} (v_g^S \otimes_S v_{gg',-1}^S) \right) \\
 &= \sum_g \left(\sum_h a_{ih} a'_{j(h^{-1}g)} \right) \cdot \mathfrak{P}^{-1} \left(\sum_{g'} v_{g'}^S \otimes_S v_{g',-1}^S \right) \\
 &= \sum_g \left(\sum_h a_{ih} a'_{j(h^{-1}g)} \right) v_g^S.
 \end{aligned}$$

Damit ist nun $k''(v_e^{S \otimes S}) =$

$$\begin{aligned}
 &= (\sigma \otimes S) (\tau \otimes S) (S \otimes \sigma^{-1}) (1 \otimes v_e^R \otimes 1) \\
 &= (\sigma \otimes S) \left(\sum_{i,j} c_{ij} \otimes 1 \otimes s_i s_j \right) \\
 &= \sum_{i,j} \left(\sum_g \sum_h (a_{ih} a'_{j(h^{-1}g)}) v_g^S \right) \otimes s_i s_j \\
 &= \sum_g \left(\sum_{i,j} \sum_h a_{ih} a'_{j(h^{-1}g)} \otimes s_i s'_j \right) v_g^{S \otimes S}.
 \end{aligned}$$

Also ist $\Gamma(k'') = \sum_g \left(\sum_i \sum_j \sum_h a_{ih} a'_{j(h^{-1}g^{-1})} \otimes s_i s'_j \right) u_g$.

Wir beenden den Beweis von (2.18.) indem wir zeigen, daß

$\Gamma(k) \Gamma(k') = \Gamma(k'')$ ist.

$$\begin{aligned}
 &\Gamma(k) \Gamma(k') = \\
 &= \left(\sum_g \sum_i (a_{ig}^{-1} \otimes s_i) u_g \right) \left(\sum_h \sum_j (a'_{jh}{}^{-1} \otimes s'_j) u_h \right) \\
 &= \sum_g \sum_i \sum_h \sum_j (a_{ig}^{-1} a'_{jh}{}^{-1} \otimes s_i s'_j) u_{gh} \\
 &= \sum_{g'} \left(\sum_i \sum_j \sum_{h'} a_{ih'} a'_{j(h'^{-1}g'^{-1})} \otimes s_i s'_j \right) u_{g'}, \\
 &= \Gamma(k'').
 \end{aligned}$$

Den quadratischen Fall betrachten wir gesondert.

(2.19.) Definition. Für eine kommutative R-Algebra

S sei $\text{Ip}(S)$ die Gruppe der Idempotenten von S. Ihre

Verknüpfung ist $e * e' = e + e' - 2 ee'$.

Wie man sieht, ist $\text{Ip}(S)$ also abelsch, das neutrale Element ist 0, und jedes Element ist zu sich selbst invers.

Indem man einem Algebrenhomomorphismus seine Einschränkung auf die Idempotenten zuordnet, erhält man einen Funktor $\text{Ip} : \underline{\text{R-Alg}} \longrightarrow \underline{\text{Ab}}$.

(2.20.) Proposition. Für die zweielementige Gruppe $C_2 = \{1, t\}$ und eine kommutative R-Algebra S sind die Zuordnungen

$$V(S[C_2]) \xrightleftharpoons{\quad} \text{Ip}(S)$$

$$s_0 \cdot 1 + s_1 t \longmapsto s_1$$

$$(1-e) \cdot 1 + et \longleftarrow e$$

zueinander inverse Isomorphismen abelscher Gruppen.

Und sie sind funktoriell in S .

Beweis. Daß sie funktoriell sind und zueinander invers, das sieht man sofort. Es genügt also zu zeigen, daß eine der Zuordnungen die Gruppenstrukturen respektiert.

Seien nun $s_0 + s_1 t, s'_0 + s'_1 t \in V(S[C_2])$. Das Produkt der Bilder in $\text{Ip}(S)$ ist dann $s_1 * s'_1 = s_1 + s'_1 - 2 s_1 s'_1$.

Andererseits wird das Produkt $(s_0 + s_1 t)(s'_0 + s'_1 t) =$

$$(s_0 s'_0 + s_1 s'_1) + (s_0 s'_1 + s_1 s'_0) t \text{ auf } s_0 s'_1 + s_1 s'_0 \text{ ab-}$$

gebildet. Die Gleichheit der beiden Ausdrücke folgt, weil

$$s_0 + s_1 = 1 = s'_0 + s'_1 \quad \text{ist (2.14.)} : s_0 s'_1 + s_1 s'_0 = \\ (1-s_1) s'_1 + s_1 (1-s'_1) = s'_1 + s_1 - 2 s_1 s'_1 .$$

(2.21.) Folgerung. Für treuflache R-Algebren S sind $Q(S/R) \simeq H^1(S/R, \text{Ip})$ funktoriell isomorphe abelsche Gruppen.

Beweis. Dies folgt aus (2.17.), (2.18.) und (2.20.).

(2.22.) Bemerkung. Orzech hat die Aussage von Satz (2.18.) mit anderen Methoden bewiesen (vgl. [35]

Theorem 3.9. und [23] S.246). Die Gruppen $V(R[G])$

— diese Bezeichnung haben wir übernommen —

treten bei ihm als erste Kohomologiegruppen auf.

Das Ergebnis (2.21.) für quadratische Erweiterung wurde auch schon von Micali und Villamayor bewiesen (vgl. [32] Chap. 2. Théorème 2). In ihrem Beweis benutzen sie Aussagen über quadratische Formen und Clifford-Algebren.

Die Interpretation von $V(R[G])$, bzw. $\text{Ip}(R)$, als Automorphismengruppe der trivialen Erweiterung zeigt wesentlich stärker als es bei den erwähnten Beweisen der Fall war, wie diese Gruppen mit der Galoisstruktur zusammenhängen. Sie gibt auch einen Anhaltspunkt dafür, wie möglicherweise Resultate vom quadratischen Fall auf beliebige Galoiserweiterungen übertragen werden können. Die Determinante von Galoiserweiterungen aus Kapitel 1 entstand zum Beispiel auf diese Weise.

Die restlichen drei Ecken des Invariantendiagrammes lassen sich kürzer abhandeln.

(2.23.) Beschreibung von $\text{Pic}(\mathcal{S}/R)$ als Gruppe verzerrter Formen.

Wollen wir Moduln ohne zusätzliche Strukturen betrachten, so nehmen wir die Struktur $\underline{M}$, deren Graph leer ist. Ist $R \hookrightarrow S$ treuflach, so bilden die verzerrten Formen des trivialen R -Moduls $R \in \underline{M}_R$ bezüglich S gerade die Menge $\text{Pic}(\mathcal{S}/R)$ (vgl. [29] Chap. 2. Prop. 8.6.). Für $T \in \underline{R}\text{-Alg}$ ist $\underline{T}\text{-Mod-aut}(T) \longrightarrow U(T)$, $f \longmapsto f(1)$ ein in T natürlicher Isomorphismus von Gruppen. (2.16.) gibt also eine Bijektion $\text{Pic}(\mathcal{S}/R) \xrightarrow{\sim} H^1(\mathcal{S}/R, U)$ an, unter der sich die Gruppenstrukturen entsprechen (vgl. [29] Chap. 1 Lemme 5.2.).

(2.24.) Beschreibung von $\text{Dis}(\mathcal{S}/R)$ als Gruppe verzerrter Formen.

Die geeignete Struktur $\underline{D}$, um Diskriminantenmoduln (vgl. 1.21.) zu beschreiben, hat offensichtlich den Graphen $2 \longrightarrow 0$ und die Funktoren $F_2^T, F_0^T : \underline{T}\text{-Mod} \longrightarrow \underline{T}\text{-Mod}$, $T \in \underline{R}\text{-Alg}$ mit $F_2^T(M) = M \otimes_T M$, $F_2^T(f) = f \otimes f$, $F_0^T(M) = T$, $F_0^T(f) = \text{id}$.

Die Menge der verzerrten Formen von $(R, 1)$ bezüglich einer treuflachen Erweiterung $R \hookrightarrow S$ stimmt mit $\text{Dis}(\mathcal{S}/R)$ überein. Dies zeigt man mit Hilfe von (2.23.) und ähnlichen Überlegungen wie bei (2.10.).

$\underline{D}_T$ -Automorphismen f von $(T, 1)$ sind T -Modulautomorphismen, welche die Bilinearstruktur erhalten. Dem entspricht die Bedingung $f(1)^2 = 1$. Wie man sieht ist also

$\underline{D}_T\text{-aut}(T, 1) \xrightarrow{\sim} \mu_2(T)$, $f \mapsto f(1)$ ein in T natürlicher Isomorphismus von Gruppen.

(2.16.) ergibt nun eine funktorielle Bijektion

$\text{Dis}(S/R) \xrightarrow{\sim} H^1(S/R, \mu_2)$. Auch sie ist wieder mit den Gruppenstrukturen verträglich ([32] Chap. 3, Théorème 3).

(2.25.) Beschreibung von $\text{Pic}(S[G]/R[G])$ als Gruppe verzerrter Formen.

G sei eine endliche abelsche Gruppe. Läßt man bei der zulässigen Struktur $\underline{G}$, welche uns zur Beschreibung von G -Galoiserweiterungen diene, die Multiplikation und die Eins weg, so erhält man eine Teilstruktur $\underline{P}$. Wir wollen nun zeigen, daß $\text{Pic}(S[G]/R[G])$ gerade aus den verzerrten $\underline{P}$ -Formen des $R[G]$ -Moduls E_R^G besteht. Wie in (2.6.) überlegt man sich: für jede R -Algebra T ist $\text{Pic}(T[G])$ eine volle isomorphie-abgeschlossene Unterkategorie von $\underline{P}_T$. $\text{Pic}(S[G]/R[G])$ ist daher eine Teilmenge der Isomorphieklassen von $\underline{P}_R$. Ist $[M] \in \text{Pic}(S[G]/R[G])$, so haben wir $S[G]$ -Modulisomorphismen $M \otimes_R S \xrightarrow{\sim} M \otimes_{R[G]} S[G] \xrightarrow{\sim} S[G] \xrightarrow{\sim} E_R^G \otimes_R S$. Also ist $[M]$ eine $\underline{P}$ -Form des $R[G]$ -Moduls E_R^G .

Sei umgekehrt $[M]$ eine $\underline{P}$ -Form von $E_R^G \in \underline{P}_R$. Wie im Beweis von Proposition (2.10.) sieht man, daß die Endomorphismen $g : M \rightarrow M$, $g \in G$ den R -Modul M zu einem $R[G]$ -Modul machen. Da $R[G] \hookrightarrow S[G]$ treuflach ist ([29] S.11) und folgende $S[G]$ -Moduln isomorph sind

$M \otimes_{R[G]} S[G] \xrightarrow{\sim} M \otimes S \xrightarrow{\sim}_{E_S^G} S[G]$, ist
 $[M] \in \text{Pic}(S[G]/R[G])$.

Man sieht mit (2.14.), daß die Gruppe der $\underline{P}_T$ -Automorphismen von E_T^G zur Einheitengruppe des Gruppenrings $T[G]$ isomorph ist. Diese Isomorphie ist funktoriell in T . (2.16.) gibt daher eine Bijektion $\text{Pic}(S[G]/R[G]) \xrightarrow{\sim} H^1(S/R, U(-[G]))$.

Orzech gibt dafür einen anderen Beweis an. Er hat bemerkt, daß die Amitsurschen Komplexe $C(S/R, U(-[G])) \xrightarrow{\sim} C(S[G]/R[G], U)$ isomorph sind [35]. Auf diese Weise erhält man auch sofort die Verträglichkeit der Bijektion mit den Gruppenstrukturen.

Daß die beiden Bijektionen übereinstimmen, läßt sich durch (längliche) Routineüberlegungen verifizieren.

§ 4 Beschreibung der Pfeile des Invarianten-Diagrammes mit Amitsurscher Kohomologie

Bevor wir darangehen, die Invarianten mit Hilfe Amitsurscher Kohomologie zu beschreiben, überzeugen wir uns zuerst davon, daß sie sich relativ einer treuflachen Erweiterung betrachten lassen.

(2.26.) Satz. Seien G eine endliche Gruppe und $R \hookrightarrow S$ eine treuflache Erweiterung. Schränkt man die

Invarianten $\det_R^G$ und dis_R^G auf $\text{Gal}(S/R, G)$ ein,
so erhält man folgendes Diagramm in $\underline{\text{Me}}^*$

$$\begin{array}{ccc} \text{Gal}(S/R) & & \\ \downarrow \text{dis}_R^G & \searrow \det_R^G & \\ \text{Dis}(S/R) & \xrightarrow{\text{vergi\ss}} & \text{Pic}(S/R) . \end{array}$$

Ist G abelsch, so entsteht aus (1.42.) das
kommutative Diagramm abelscher Gruppen

$$\begin{array}{ccc} \text{Gal}(S/R, G) & \xrightarrow{\text{pic}_R^G} & \text{Pic}(S[G]/R[G]) \\ \downarrow \text{dis}_R^G & \searrow \det_R^G & \downarrow \text{sign}^* \\ \text{Dis}(S/R) & \xrightarrow{\text{vergi\ss}} & \text{Pic}(S/R) . \end{array}$$

Beweis. Es ist nur nachzuweisen, daß die eingeschränkten Invarianten ihre Werte in den angegebenen Mengen annehmen. Für pic_R^G und $\text{vergi\ss}$ ist das klar
Sei $[P] \in \text{Pic}(S[G]/R[G])$. Dann sind folgende S -Moduln
isomorph $P \otimes_{R[G]} (\text{sign}^R) \otimes_R S \simeq (P \otimes_R S) \otimes_{S[G]} (\text{sign}^S)$
 $\simeq S[G] \otimes_{S[G]} (\text{sign}^S) \simeq S$. Also ist $\text{sign}^*([P]) \in \text{Pic}(S/R)$.

Es ist also noch zu zeigen, daß $\text{dis}_R^G(\text{Gal}(S/R, G))$ in $\text{Dis}(S/R)$ liegt.

Sei $[B] \in \text{Gal}(S/R, G)$.

Die Inklusion $B^{\text{sign}} \otimes S \hookrightarrow (B \otimes S)^{\text{sign}}$ ist klar. Wir
tensorieren sie mit der treuflachen Erweiterung $S \hookrightarrow B \otimes S$
und erhalten folgendes kommutative Diagramm

$$\begin{array}{c}
 \text{inkl} \otimes (B_S) \\
 \text{S} \\
 (B^{\text{sign}} \otimes S) \otimes (B \otimes S) \xrightarrow{\quad} (B \otimes S)^{\text{sign}} \otimes (B \otimes S) \\
 \downarrow \text{kan} \\
 (B^{\text{sign}} \otimes B) \otimes S \xrightarrow{\quad} (B \otimes B) \otimes S \xrightarrow{\sim} (B_S) \otimes (B_S) \quad (*) \\
 \downarrow \nabla \otimes S \quad \downarrow \nabla_S \\
 (B \otimes S) \xrightarrow{\sim} B_S
 \end{array}$$

In (1.13.) haben wir gezeigt, daß die mit (*) gekennzeichneten Pfeile Isomorphismen sind. $\text{inkl} \otimes (B_S)$ ist also bijektiv, und folglich ist dies auch $\text{inkl} : B^{\text{sign}} \otimes S \xrightarrow{\sim} (B \otimes S)^{\text{sign}}$. Diese Bijektion ist mit den Bilinearformen verträglich, wie ein Blick auf das Diagramm zeigt. Außerdem sind $((B \otimes S)^{\text{sign}}, \text{mult}) \xrightarrow{\sim} \xrightarrow{\sim} (E_S^G)^{\text{sign}}, \text{mult}) \xrightarrow{\sim} (S, 1)$ isomorphe Diskriminantenmoduln.

Also ist $\text{dis}_R^G([B]) \in \text{Dis}(S/R)$.

(2.26.1.)

Es sei noch kurz angedeutet, wie der zuletzt genannte Isomorphismus zustande kommt. Dazu prüft man nach, daß das Element $\sum_g \text{sign}(g) v_g \in E_S^G$ ein freies S-Erzeugendensystem von $(E_S^G)^{\text{sign}}$ bildet. Da $(\sum_g \text{sign}(g) v_g)^2 = 1$ ist, ist $S \ni s \mapsto s(\sum_g \text{sign}(g) v_g) \in (E_S^G)^{\text{sign}}$ ein Isomorphismus der Diskriminantenmoduln $(S, 1) \xrightarrow{\sim} ((E_S^G)^{\text{sign}}, \text{mult})$.

Um die Diagramme von (2.26.) durch Amitsur-Kohomologie

beschreiben zu können, benötigen wir nun noch geeignete gruppenwertige Funktoren. Als Vorbereitung dazu betrachten wir ein Diagramm von Automorphismengruppen.

(2.27.) Indem man bei der G -Galoiserweiterung E_R^G zunächst die Multiplikation, dann auch die G -Struktur vergißt, erhält man eine aufsteigende Folge von Automorphismengruppen. Daraus entsteht das folgende Diagramm: (Man beachte, daß die endliche Gruppe G hier nicht abelsch sein muß.)

$$\begin{array}{ccccc}
 \text{Gal}(R, G) \text{-aut}(E_R^G) & \hookrightarrow & R[G] \text{-Mod-aut}(E_R^G) & \hookrightarrow & R \text{-Mod-aut}(E_R^G) \\
 \Gamma \downarrow \wr & & \Gamma \downarrow \wr & & \text{kan} \downarrow \wr \\
 V(R[G]) & \xrightarrow{\text{pic}} & U(R[G]) & \xrightarrow{\nu} & GL(n, R) \\
 & & \downarrow \text{sign} & \swarrow \text{det} & \\
 \mu_2(R) & \xrightarrow{\text{inkl}} & U(R) & &
 \end{array}$$

Γ ist aus (2.14.); pic, ν seien von den darüberstehenden Inklusionen induziert; det sei die gewöhnliche Determinantenabbildung von Matrizen; sign werde durch sign_R^G induziert.

Die Bezeichnungen pic, sign sollen schon auf die enge Verbindung mit den Invarianten hinweisen. Dies läßt sich noch weiter treiben, wie wir sogleich sehen werden.

(2.28.) Proposition. Im soeben konstruierten Diagramm gilt a.) $\text{sign pic} = \det \nu \text{ pic}$

b.) sign pic faktorisiert über $\mu_2(R)$.

(2.29.) Bezeichnung. Wir nennen den Homomorphismus $\text{sign pic} : V(R[G]) \longrightarrow U(R)$ ebenfalls "Determinante" und seine Faktorisierung $V(R[G]) \longrightarrow \mu_2(R)$ "Diskriminante".

Das Gegenstück zu (2.26.) ist damit

$$\begin{array}{ccc}
 V(R[G]) & \xrightarrow{\text{pic}} & U(R[G]) \\
 \text{dis} \downarrow & \searrow \text{det} & \downarrow \text{sign} \\
 \mu_2(R) & \xrightarrow{\text{inkl}} & U(R)
 \end{array}$$

Allerdings braucht G hier nicht abelsch zu sein.

Beweis von (2.28.). a.) Sei $f : E_R^G \longrightarrow E_R^G$ ein

$\text{Gal}(R, G)$ -Automorphismus, und es sei $f(v_e) = \sum_g r_g v_g$.

Es gilt dann $f(v_h) = \sum_g r_g v_{hg} = \sum_g r_h^{-1} v_g$. Bezüg-

lich der Basis $\{v_g \mid g \in G\}$ wird f also durch die Matrix dargestellt, welche im Schnittpunkt der Spalte h mit der Zeile g das Element $r_h^{-1} v_g$ stehen hat. Deshalb ist $\det \nu \text{ pic}(\sum_g r_g^{-1} u_g) = \det \text{kan}(f) =$

$= \sum_{\pi \in S_n} \varepsilon(\pi) \prod_{g \in G} r_g^{-1} \pi(g)$. (n ist dabei die Ordnung von G .)

Da die r_g paarweise orthogonal sind, ist

$\prod_{g \in G} r_g^{-1} \pi(g)$ nur dann von 0 verschieden, wenn

die Permutation π eine Rechtstranslation

$G \ni g \longmapsto gh \in G, h \in G$ ist. Betrachtet man den Be-

weis von Proposition (1.17.), so erkennt man, daß

das die Vorzeichen von Rechts- und Linkstransla-

tion eines Elementes h übereinstimmen.

Es gilt also weiter

$$\begin{aligned} \det \nu \text{pic} \left(\sum_g r_g^{-1} u_g \right) &= \sum_{h \in G} \text{sign}_R^G(h) r_h = \\ &= \sum_{h \in G} \text{sign}_R^G(h^{-1}) r_h = \text{sign} \left(\sum_g r_g^{-1} u_g \right). \end{aligned}$$

$$\begin{aligned} \text{b.) Sei } \sum_g r_g u_g &\in V(R[G]). \quad (\text{sign pic} \left(\sum_g r_g u_g \right))^2 = \\ &= \left(\sum_g \text{sign}(g) r_g \right) \left(\sum_h \text{sign}(h) r_h \right) = \sum_g \text{sign}(g)^2 r_g = 1. \end{aligned}$$

Wir wollen nun zeigen, daß die Homomorphismen zwischen den Automorphismengruppen auf den Mengen der verzerrten Formen gerade die entsprechenden Invarianten induzieren.

Für einen Teil davon geben wir einen abstrakten Beweis

an. Die abstrakt formulierte Aussage können wir mehr-

mals anwenden, und der Umfang der neu einzuführenden

Terminologie hält sich in Grenzen.

(2.30.) Definition. Sei $\underline{A}$ eine zulässige Struktur mit dem Graphen $\underline{A}$ und Familien $(F_x^S), (\phi_x^q)$ (vgl. 2.5.).

Sei $\underline{B}$ ein Untergraph von $\underline{A}$, d.h. $\dot{B} \subseteq \dot{A}$, $\vec{B} \subseteq \vec{A}$ sind Teilmengen, und die Quell- und Zielabbildungen von $\underline{B}$ sind Einschränkungen der entsprechenden Abbildungen von $\underline{A}$. Dann bildet $\underline{B}$ zusammen mit den Teilfamilien $(F_x^S \mid x \in \dot{B}, S \in \underline{R-Alg})$, $(\phi_x^q \mid x \in \dot{B}, q \in \underline{R-Alg})$ eine zulässige Struktur $\underline{B}$. Solch eine Struktur $\underline{B}$ nennen wir "Unterstruktur" von $\underline{A}$.

(2.31.) Bemerkungen. Sei $\underline{B}$ eine Unterstruktur von $\underline{A}$. Folgende Aussagen ergeben sich unmittelbar aus der Definition:

a.) Bezeichnet $U : \underline{B} \hookrightarrow \underline{A}$ die Einbettung, so ist für jede R -Algebra T ein Funktor

$$\begin{aligned} \underline{A}_T &\longrightarrow \underline{B}_T \\ (A, \mathcal{A}) &\longmapsto (A, \mathcal{A}U) \\ f &\longmapsto f \end{aligned}$$

gegeben.

b.) Seien $(A, \mathcal{A}) \in \underline{A}_R$ und $R \hookrightarrow S$ treuflach. Dann ist die Zuordnung

$V_{\underline{A}}^S(A, \mathcal{A}) \ni [B, \mathcal{B}] \longmapsto [B, \mathcal{B}U] \in V_{\underline{B}}^S(A, \mathcal{A}U)$ wohldefiniert und erhält die Punktierung. Außerdem gilt :

$\underline{A}_S\text{-aut}(A_S, \mathcal{A}_S) \hookrightarrow \underline{B}_S\text{-aut}(A_S, \mathcal{A}_S)$ ist eine Untergruppe, und die Einbettung ist funktoriell in S .

(2.32.) Satz. Seien $\underline{B}$ eine Unterstruktur einer zulässigen Struktur $\underline{A}$, $(A, \mathcal{A}) \in \underline{A}_R$ und $R \hookrightarrow S$ eine

treuflache Erweiterung. Dann kommutiert das Diagramm

$$\begin{array}{ccc}
 v_{\underline{A}}^S(A, \mathcal{A}) & \longrightarrow & v_{\underline{B}}^S(A, \mathcal{A}U) \\
 \downarrow \wr & & \downarrow \wr \\
 H^1(S/R, \underline{\text{Aut}}(A, \mathcal{A})) & \longrightarrow & H^1(S/R, \underline{\text{Aut}}(A, \mathcal{A}U))
 \end{array}$$

Die senkrechten Pfeile sind die Bijektionen aus (2.16.), die waagrechten Pfeile sind in (2.31.) beschrieben.

Beweis. Sei $[B, \mathcal{B}]$ eine verzerrte $\underline{A}$ -Form von $(A, \mathcal{A})$ bezüglich S . Sei $\beta : (B_S, \mathcal{B}_S) \xrightarrow{\sim} (A_S, \mathcal{A}_S)$ ein $\underline{A}_S$ -Isomorphismus. Beide Wege schicken $[B, \mathcal{B}]$ auf den 1-Kozykel $d_2^*(\beta)d_1^*(\beta)^{-1} \in \underline{B}_S \otimes_S \text{-aut}(A_S \otimes_S, \mathcal{A}_U \otimes_S)$.

(2.33.) Folgerungen. $R \hookrightarrow S$ sei treuflach.

a.) Folgendes Diagramm ist kommutativ

$$\begin{array}{ccc}
 \text{Dis}(S/R) & \xrightarrow{\text{vergi\ss}} & \text{Pic}(S/R) \\
 \downarrow \wr & & \downarrow \wr \\
 H^1(S/R, \mu_2) & \xrightarrow{H^1(S/R, \text{inkl})} & H^1(S/R, U)
 \end{array}$$

b.) Ist die endliche Gruppe G abelsch, so kommutiert

$$\begin{array}{ccc}
 \text{Gal}(S/R, G) & \xrightarrow{\text{pic}_R^G} & \text{Pic}(S[G]/R[G]) \\
 \downarrow \wr & & \downarrow \wr \\
 H^1(S/R, V(-[G])) & \xrightarrow{H^1(S/R, \text{pic})} & H^1(S/R, U(-[G])).
 \end{array}$$

Beweis. Mit den Bezeichnungen von (2.23.), (2.24.), (2.25.) ist $\underline{M}$ eine Teilstruktur von $\underline{D}$, und $\underline{P}$ ist eine Teilstruktur von $\underline{G}$.

(2.34.) Bemerkung. Beim Beweis der entsprechenden Aussagen für dis_R^G und sign^* kommt man nicht mehr mit (2.32.) aus. Wollte man eine abstrakte Version beweisen, welche auch diese Fälle umfaßt, so müßte man Morphismen zulässiger Strukturen einführen.

Vor allem durch Verträglichkeitsbedingungen bezüglich Skalarbereichserweiterungen ergäbe sich dabei aber ein derart aufgeblasener Begriffsapparat, daß wir davon absehen und für die verbleibenden zwei Fälle direkte Beweise angeben.

(2.35.) Satz. Seien G eine endliche Gruppe und $R \hookrightarrow S$ eine treuflache Erweiterung.

Folgendes Diagramm kommutiert

$$\begin{array}{ccc} \text{Gal}(S/R, G) & \xrightarrow{\text{dis}_R^G} & \text{Dis}(S/R) \\ \downarrow \wr & & \downarrow \wr \\ H^1(S/R, V(-[G])) & \xrightarrow{\quad} & H^1(S/R, \mu_2) \\ & H^1(S/R, \text{dis}) & \end{array}$$

Beweis. Seien B eine G -Galoiserweiterung von R und

$\beta: B_S \longrightarrow E_S^G$ ein $\text{Gal}(S, G)$ -Isomorphismus. Die verzerrte Form $[B]$ entspricht der Klasse des Kozykels

$k := d_2^*(\beta) d_1^*(\beta)^{-1}$. k ist ein Automorphismus

$E_S^G \otimes S \longrightarrow E_S^G \otimes S$. Ist $k(v_e) = \sum s_g v_g$, so ist

$$\Gamma(k) = \sum s_g^{-1} u_g \quad \text{und} \quad \text{dis } \Gamma(k) = \\ = \sum_g \text{sign}(g) s_g \in \mu_2(S \otimes S) \quad (\text{vgl. 2.28.}).$$

Nun ist zu zeigen, daß man auf dem anderen Weg einen komologen Kozykel erhält.

Sei $\lambda : B^{\text{sign}} \otimes S \xrightarrow{\sim} S$ der Dis(S)-Isomorphismus gemäß (2.16.). Dann ist der zugehörige 1-Kozykel $d_2^*(\lambda) d_1^*(\lambda)^{-1}$. Der Übergang von Dis(S ⊗ S)-aut(S ⊗ S, 1) zu $\mu_2(S \otimes S)$ geschieht durch Auswerten bei $1 \otimes 1$. Im folgenden zeigen wir sogar: $\sum_g \text{sign}(g) s_g = d_2^*(\lambda) d_1^*(\lambda)^{-1} (1 \otimes 1)$.

Dazu betrachten wir das Diagramm

$$\begin{array}{ccccc} S \otimes S & \xrightarrow{S \otimes \pi} & S \otimes (E_R^G \otimes S)^{\text{sign}} & \xrightarrow{\quad} & S \otimes (B \otimes S)^{\text{sign}} \\ & & \searrow & & \parallel \\ & & S \otimes \lambda^{-1} & \searrow & S \otimes B^{\text{sign}} \otimes S \\ & & \downarrow k & & \parallel \tau \otimes S \\ & & \lambda \otimes S & \searrow & B^{\text{sign}} \otimes S \otimes S \\ & & \downarrow & & \parallel \\ S \otimes S & \xleftarrow{\pi^{-1} \otimes S} & (E_R^G \otimes S)^{\text{sign}} \otimes S & \xleftarrow{\quad} & (B \otimes S)^{\text{sign}} \otimes S. \end{array}$$

(π ist dabei der Isomorphismus aus (2.26.1.)). In ihm gilt:

$$d_2^*(\lambda) d_1^*(\lambda)^{-1} (1 \otimes 1) = \\ = (\pi^{-1} \otimes S) k (S \otimes \pi) (1 \otimes 1) \\ = (\pi^{-1} \otimes S) k \left(\sum_h \text{sign}(h) \cdot 1 \otimes v_h^R \otimes 1 \right)$$

$$\begin{aligned}
 &= (\pi^{-1} \otimes S) \left(\sum_h \text{sign}(h) h \cdot k(1 \otimes v_e \otimes 1) \right) \\
 &= (\pi^{-1} \otimes S) \left(\sum_h \sum_g \text{sign}(h) s_g v_{hg}^{S \otimes S} \right) \\
 &= (\pi^{-1} \otimes S) \left(\sum_h \sum_g \text{sign}(g) s_g \text{sign}(hg) v_{hg} \right) \\
 &= (\pi^{-1} \otimes S) \left(\left(\sum_g \text{sign}(g) s_g \right) \left(\sum_h \text{sign}(h) v_h \right) \right) \\
 &= \sum_g \text{sign}(g) s_g.
 \end{aligned}$$

(2.36.) Folgerung. In der Situation des Satzes kommutiert auch das Diagramm

$$\begin{array}{ccc}
 \text{Gal}(S/R, G) & \xrightarrow{\det_R^G} & \text{Pic}(S/R) \\
 \downarrow \wr & & \downarrow \wr \\
 H^1(S/R, V(-[G])) & \xrightarrow{H^1(S/R, \det)} & H^1(S/R, U)
 \end{array}$$

Beweis. Dies folgt aus den kommutativen Diagrammen (2.26.), (2.29.), (2.33.), (2.35.).

(2.37.) Folgerung. Im Fall der quadratischen Erweiterungen nimmt die Diskriminante der Automorphismengruppen bei $S \in R\text{-Alg}$ folgende Gestalt an (vgl. 2.20; 2.27.)

$$\begin{aligned}
 \text{Ip}(S) &\xrightarrow{\sim} V(S[C_2]) \xrightarrow{\text{dis}} \mu_2(S) \\
 e &\longmapsto (1-e) + et \longmapsto 1-2e.
 \end{aligned}$$

Das Diagramm von (2.35.) wird zu

$$\begin{array}{ccc} \mathcal{Q}(S/R) & \xrightarrow{\text{dis}_R^{C_2}} & \text{Dis}(S/R) \\ \wr & & \wr \\ H^1(S/R, \text{Ip}) & \xrightarrow{H^1(S/R, \text{dis})} & H^1(S/R, \mu_2). \end{array}$$

Dasselbe Resultat erzielten Micali und Villamayor ([33] 2.3.) mit ganz anderen Methoden.

(2.38.) Satz. Seien G eine endliche abelsche Gruppe und $R \hookrightarrow S$ eine treuflache Erweiterung. Dann kommutiert das Diagramm

$$\begin{array}{ccc} \text{Pic}(S[G]/R[G]) & \xrightarrow{\text{sign}^*} & \text{Pic}(S/R) \\ \wr & & \wr \\ H^1(S/R, U(-[G])) & \xrightarrow{H^1(S/R, \text{sign})} & H^1(S/R, U) \end{array}.$$

Beweis. Wir gehen wie im Beweis von (2.35.) vor. Sei P ein invertierbarer $R[G]$ -Modul, und sei $\beta: P_S \longrightarrow S[G]$ ein Isomorphismus von $S[G]$ -Moduln. $[P]$ entspricht dann der Klasse von $k := d_2^*(\beta) d_1^*(\beta)^{-1}$. k ist ein Automorphismus von $S \otimes S[G]$. Deshalb ist $k(u_e) \in U(S \otimes S[G])$. Sei $k(u_e) = : \sum_g s_g u_g$. Dann ist $H^1(S/R, \text{sign})[k] = [\text{sign } k(u_e)] = [\sum_g \text{sign}(g) s_g]$.

Sei $\alpha: \text{sign}^*(P) \otimes S \longrightarrow S$ der S -Modulisomorphismus aus (2.26.). Wir zeigen nun, daß $d_2^*(\alpha) d_1^*(\alpha)^{-1} (1 \otimes 1) = \sum_g \text{sign}(g) s_g$ ist. Dazu betrachten wir folgendes Dia-

gramm von $(S \otimes S)$ -Modulisomorphismen

$$\begin{array}{ccc}
 S \otimes S & \xrightarrow{\text{kan}^{-1}} & (S \otimes S[G]) \quad (S \otimes S)[G] \quad (\text{sign } S \otimes S) \\
 \downarrow S \otimes \alpha^{-1} & & \downarrow (S \otimes \beta^{-1}) \otimes (\text{sign } S \otimes S) \\
 S \otimes \text{sign}^*(P) \otimes S & \xrightarrow{\sim} & (S \otimes P \otimes S) \quad (S \otimes S)[G] \quad (\text{sign } S \otimes S) \\
 \downarrow \tau \otimes S & & \downarrow (\tau \otimes S) \otimes (\text{sign } S \otimes S) \\
 \text{sign}^*(P) \otimes S \otimes S & \xrightarrow{\sim} & (P \otimes S \otimes S) \quad (S \otimes S)[G] \quad (\text{sign } S \otimes S) \\
 \downarrow S \otimes \alpha & & \downarrow (\beta \otimes S) \otimes (\text{sign } S \otimes S) \\
 S \otimes S & \xleftarrow{\text{kan}} & (S[G] \otimes S) \quad (S \otimes S)[G] \quad (\text{sign } S \otimes S)
 \end{array}$$

Das Diagramm kommutiert, und die Komposition der senkrechten Pfeile auf der rechten Seite ergibt

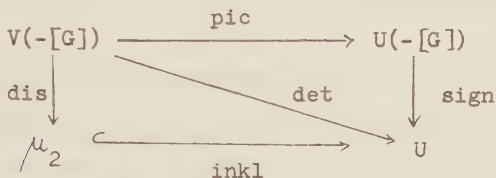
$k \otimes (\text{sign } S \otimes S)$. Deshalb gilt

$$\begin{aligned}
 & d_2^*(\alpha) d_1^*(\alpha)^{-1} (1 \otimes 1) \\
 &= \text{kan} \quad (k \otimes (\text{sign } S \otimes S)) \quad \text{kan}^{-1} \cdot (1 \otimes 1) \\
 &= \text{kan} \quad (k \otimes \text{id}) \quad (1 \otimes u_e \otimes 1) \\
 &= \text{kan} \quad ((\sum_g s_g u_g) \otimes 1) \\
 &= \sum_g \text{sign}(g) s_g.
 \end{aligned}$$

Damit ist das Ziel dieses Paragraphen erreicht: Wir können die Invarianten-Diagramme aus (2.26.) mit Amitsurs Kohomologie beschreiben.

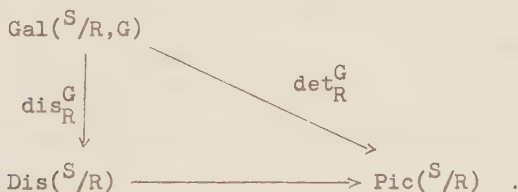
(2.39.) Zusammenfassung. Für eine endliche Gruppe

G ist

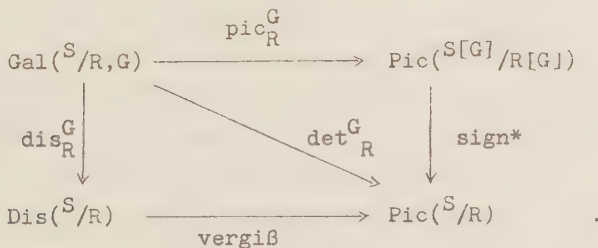


ein kommutatives Diagramm gruppenwertiger Funktoren.

Ist $R \hookrightarrow S$ treuflach, so macht die erste Amitsursche Kohomologie $H^1(S/R, -)$ aus dem linken Dreieck folgendes kommutative Dreieck in $\underline{\text{Me}}^*$ (vgl. 2.26.)



Ist G abelsch, so sind die betrachteten Funktoren abelschwertig, und für eine treuflache Erweiterung $R \hookrightarrow S$ macht $H^1(S/R, -)$ daraus folgendes kommutative Diagramm in $\underline{\text{Ab}}$ (vgl. 2.26.)



§ 5 Beschreibung des Invarianten-Diagrammes mit Čechscher Kohomologie

Bisher haben wir nur die Einschränkungen der Invarianten bezüglich treuflacher Erweiterungen $R \hookrightarrow S$ kohomologisch beschrieben. Durch Übergang zu einem geeigneten Kolimes wollen wir daraus nun eine Beschreibung der gesamten Invarianten gewinnen.

Dabei geht es nicht darum, die Invarianten als Abbildungen zwischen Vereinigungen von Kozykel-Mengen darzustellen. Die Bedeutung der folgenden Überlegungen liegt darin, daß die Invarianten als Ganzes im Rahmen einer Kohomologietheorie beschrieben werden.

Die Čechsche Kohomologietheorie erfordert einen sehr umfangreichen Begriffsapparat. Wir erinnern an dieser Stelle nur an die grundlegenden Begriffe und die wichtigsten Eigenschaften davon. Außerdem vereinbaren wir einige Bezeichnungen, welche in dem von uns betrachteten Spezialfall günstig sind. Ansonsten verwenden wir die Terminologie von Artin [2].

(2.40.0.) Zuerst wollen wir auf eine Eigentümlichkeit hinweisen, die in der Literatur meistens übergangen wird. Da Funktorkategorien mit nicht-kleiner Quell-Kategorie betrachtet werden, legt man eine durch Universen ergänzte Mengenlehre zugrunde. Alle üblichen Kategorien wie R-Alg, Gal(R,G), Ab, Me liegen dann in einem "Grund-Universum", Funktorkategorien wie Funkt (R-Alg, Ab) liegen

in einem höheren Universum

Auch die — im ersten Augenblick überraschende — Bildung von Limites über nicht-kleinen Indexkategorien wird zunächst in einem höheren Universum vollzogen. Anschließend wird dann meistens gezeigt, daß die so konstruierten Limites doch bereits im "Grund-Universum" liegen.

(2.40.1.) Definition der treuflachen Topologie.

Wir wählen eine für unsere Zwecke geeignete Grothendieck-Topologie, im Sinn von Artin [2] .

Die zugrundeliegende Kategorie sei $\underline{R\text{-Alg-tf}}^{\text{op}}$.

Überdeckungen eines Objektes S seien einpunktige Mengen $\{S \hookrightarrow T\}$, so daß T eine endlich erzeugte (als Algebra) treuflache S -Algebra ist.

Man überzeugt sich schnell, daß dies eine Grothendieck-Topologie ist. Wir nennen sie "treuflache Topologie" und schreiben dafür $\mathcal{T}_R$.

(2.40.2.) Definition von Prägarben und Garben.

Eine Prägarbe über $\mathcal{T}_R$ ist ein Funktor

$F : \underline{R\text{-Alg-tf}} \longrightarrow \underline{\text{Ab}}$. F heißt Garbe, wenn für jede

Überdeckung $q : S \longrightarrow T$ das Diagramm

$$0 \longrightarrow F(S) \xrightarrow{F(q)} F(T) \xrightarrow[\begin{smallmatrix} F(d_2) \\ \searrow \end{smallmatrix}]{\begin{smallmatrix} F(d_1) \\ \nearrow \end{smallmatrix}} F(T \otimes_S T) \quad \text{exakt ist.}$$

Die Kategorie der Prägarben über $\mathcal{T}_R$ und der funk-

toriellen Morphismen bezeichnen wir mit $\mathcal{Q}$. Für die volle Unterkategorie der Garben auf $\mathcal{G}_R$ schreiben wir $\mathcal{S}$.

(2.40.3.) Eigenschaften von $\mathcal{Q}$.

Die Kategorie der Prägarben über der treuflachen Topologie ist abelsch und hat "genügend Injektive" (vgl. [2] S.14, S.17). Deshalb sind die Ergebnisse aus Grothendiecks Tôhoku-Artikel [25] anwendbar:

Für jeden linksexakten Funktor $L : \mathcal{Q} \longrightarrow \underline{\text{Ab}}$ bilden die, mit Hilfe injektiver Auflösungen konstruierten, abgeleiteten Funktoren $D^i L$, $i \geq 0$ einen exakten universellen $\mathcal{Q}$ -Funktor, der in der 0 -ten Dimension mit L übereinstimmt. Bis auf Isomorphie ist dies auch der einzige $\mathcal{Q}$ -Funktor, welcher exakt, universell und in der 0 -ten Dimension gleich L ist.

Wir verzichten hier darauf, die Definitionen all dieser Begriffe wiederzugeben. Doch sei bemerkt, daß die Exaktheit in $\mathcal{Q}$ punktweise zu verstehen ist, d.h. eine Folge $F' \xrightarrow{\pi} F \xrightarrow{\pi'} F''$ von Prägarben ist genau dann exakt, wenn für jede treuflache R -Algebra S die Folge

$$F'(S) \xrightarrow{\pi(S)} F(S) \xrightarrow{\pi(S)} F''(S)$$

exakt ist.

(2.40.4.) Eigenschaften der Kategorie $\mathcal{S}$.

Auch $\mathcal{S}$ ist abelsch und hat genügend Injektive. Der Vergißfunktor $\iota : \mathcal{S} \longrightarrow \mathcal{P}$ besitzt den Linksadjungierten "assozierte Garbe" $\# : \mathcal{P} \longrightarrow \mathcal{S}$ [2]. ι erhält, wegen der Adjungiertheit, Limites. Insbesondere ist ι linksexakt. Vom Funktor $\#$ kann man sogar zeigen, daß er exakt ist. Produkte und Kerne werden in $\mathcal{S}$ also punktweise gebildet, Kokerne im allgemeinen jedoch nicht.

(2.40.5.) Definition der Čech-Kohomologie.

Da die Überdeckungen der treuflachen Topologie von besonders einfacher Form sind, vereinfacht sich auch die Beschreibung der Čechschen Kohomologiegruppen.

Sei F eine Prägarbe und $n \geq 0$.

Für jede Überdeckung $\{R \hookrightarrow S\}$ von R bilden wir die Amitsursche Kohomologiegruppe $H^n(S/R, F)$ (vgl. 2.12.).

Nun hat die Amitsur-Kohomologie bekanntlich die Eigenschaft, daß für je zwei R -Algebrenhomomorphismen

$q, q' : S \longrightarrow T$ die Morphismen $H^n(q/R, F) = H^n(q'/R, F)$ übereinstimmen.

Den Kolimes der $H^n(S/R, F)$ über alle Überdeckungen von R können wir daher folgendermaßen bilden:

Sei Ω_R die Menge der Isomorphieklassen von Überdeckungen von R . (Ω_R ist tatsächlich eine Menge,

da jede Überdeckung als R -Algebra endlich erzeugt ist, und ihre Kardinalität daher nicht größer als $\text{card}(R) + \aleph_0$ sein kann.) Wir versehen Ω_R mit einer Relation, und zwar sei $[S] \leq [T] : \iff R\text{-Alg}(S, T) \neq \emptyset$. Diese Relation ist reflexiv, transitiv, und für je zwei Elemente $[S], [T] \in \Omega_R$ gibt es eine gemeinsame Majorante $[S \otimes T]$. Deshalb ist $\varinjlim : \text{Funkt}(\Omega_R, \text{Ab}) \longrightarrow \text{Ab}$ exakt ([2] Cor. 1.4.), und über Ω_R werden Kolimites abelscher Gruppen wie in den Mengen gebildet ([2] Prop. 1.3.).

Wie wir schon vorher überlegten, ist

$H^n(-/R, F) : \Omega_R \longrightarrow \text{Ab}$ ein Funktor.

$$\check{H}^n(R, F) := \varinjlim_{\Omega_R} H^n(S/R, F)$$

ist die n -te Čechsche Kohomologiegruppe von F bezüglich der treuflachen Topologie.

(2.40.6.) Eigenschaften der Čechschen Kohomologie.

Die $\check{H}^n(R, -)$ sind auf naheliegende Weise Funktoren

$\mathcal{P} \longrightarrow \text{Ab}$. Ihre entscheidende Eigenschaft ist:

$\check{H}^0(R, -) : \mathcal{P} \longrightarrow \text{Ab}$ ist linksexakt, und die

$\check{H}^n(R, -)$, $n \geq 0$ sind die abgeleiteten Funktoren davon ([2] S.37).

Es sei noch eine Bemerkung angefügt, die später oft nützlich sein wird.

Hat eine Prägarbe F die Eigenschaft (+)
 " für jede Überdeckung $q : S \longrightarrow T$ in $\mathcal{C}_R$ ist
 $F(q) : F(S) \longrightarrow F(T)$ injektiv", so ist
 $\check{H}^0(R, F) = F^\#(R)$.

Da Garben offensichtlich die Eigenschaft (+) be-
 sitzen, ist $\check{H}^0(R, -) : \mathcal{C} \longrightarrow \underline{\text{Ab}}$ die Auswertung
 an der Stelle R .

Mit diesen Methoden gehen wir nun daran, die
 Aufgabe zu erfüllen, welche wir uns im Titel von
 Kapitel 2 gestellt haben.

(2.41.) Satz. Seien R ein kommutativer Ring und
 G eine endliche abelsche Gruppe.

Dann ist

$$\begin{array}{ccc}
 V(-[G]) & \xrightarrow{\text{pic}} & U(-[G]) \\
 \text{dis} \downarrow & \searrow \text{det} & \downarrow \text{sign} \\
 \mu_2 & \xrightarrow{\text{inkl}} & U
 \end{array}$$

ein kommutatives Diagramm von Prägarben über der
 treuflachen Topologie $\mathcal{C}_R$ (vgl. 2.39.). Die Čechschen
 Kohomologiefunktoren $\check{H}^0(R, -)$, $\check{H}^1(R, -)$ machen daraus
 folgende kommutativen Diagramme abelscher Gruppen

$$\begin{array}{ccc}
 V(R[G]) & \xrightarrow{\text{pic}} & U(R[G]) \\
 \downarrow \text{dis} & \searrow \text{det} & \downarrow \text{sign} \\
 \mu_2(R) & \xrightarrow{\text{inkl}} & U(R)
 \end{array}
 \qquad
 \begin{array}{ccc}
 \text{Gal}(R, G) & \xrightarrow{\text{pic}_R^G} & \bigcup \text{Pic}(S[G]/R[G]) \\
 \downarrow \text{dis}_R^G & \searrow \text{det}_R^G & \downarrow \text{sign}^* \\
 \text{Dis}(R) & \xrightarrow{\text{vergi\ss}} & \text{Pic}(R)
 \end{array}$$

Beweis. Wenden wir uns zuerst $\check{H}^1(R, -)$ zu.

$$\begin{aligned}
 \check{H}^1(R, V(-[G])) &= \varinjlim_{\Omega_R} H^1(S/R, V(-[G])) \\
 &\simeq \varinjlim_{\Omega_R} \text{Gal}(S/R, G)
 \end{aligned}$$

wissen wir aus (2.39.). Einer Relation $[S] \triangleleft [T]$ in Ω_R entspricht ein Morphismus $\text{Gal}(S/R, G)$ für ein $q \in \underline{\text{R-Alg}}(S, T)$. Wie bei allen Mengen verzerrter Formen ist dies jedoch einfach die Inklusion

$$\begin{aligned}
 \text{Gal}(S/R, G) &\hookrightarrow \text{Gal}(T/R, G) \quad (2.7.). \text{ Daher ist} \\
 \varinjlim_{\Omega_R} \text{Gal}(S/R, G) &= \bigcup_{\Omega_R} \text{Gal}(S/R, G).
 \end{aligned}$$

Auf dieselbe Weise ergeben sich Isomorphismen

$$\begin{aligned}
 \check{H}^1(R, U) &\simeq \bigcup_{\Omega_R} \text{Pic}(S/R) \\
 \check{H}^1(R, \mu_2) &\simeq \bigcup_{\Omega_R} \text{Dis}(S/R) \\
 \check{H}^1(R, U(-[G])) &\simeq \bigcup_{\Omega_R} \text{Pic}(S[G]/R[G]).
 \end{aligned}$$

Für die ersten Čechschen Kohomologiegruppen ist

(2.41.) also bewiesen, wenn wir zeigen, daß die jeweiligen Vereinigungen mit $\text{Gal}(R, G)$, $\text{Pic}(R)$ und $\text{Dis}(R)$ übereinstimmen.

Chase und Rosenberg zeigen, daß für $[P] \in \text{Pic}(R)$ eine "Zariski-Überdeckung" $R \hookrightarrow S$ existiert, mit $[P] \in \text{Pic}(S/R)$ (vgl. [13] Th.5.2.; [29] I.5.1.). Ist $[P, \alpha] \in \text{Dis}(R)$ und $\pi: S \xrightarrow{\sim} P_S$ ein S -Modul-isomorphismus für eine Zariski-Überdeckung $R \hookrightarrow S$, so ist $[P, \alpha] \in \text{Dis}(S/R)$, falls $u := \alpha_S(\pi \otimes \pi)(1 \otimes 1) \in U^2(S)$ ist. Ansonsten geht man zur Erweiterung $S[x]/(x^2 - u)$ über.

Zu $\bigcup_R \text{Pic}(S[G]/R[G])$ sei angemerkt, daß die Vereinigung nur über Erweiterungen $R[G] \ni \sum r_g u_g \mapsto \sum j(r_g) u_g \in S[G]$ gebildet wird, wobei $j: R \hookrightarrow S$ endlich erzeugt und treuflach ist. Es sind also nicht nur die Algebren, sondern auch die Einbettungen vorgeschrieben.

Was $\text{Gal}(R, G)$ betrifft, so geben wir zu einer G -Galoiserweiterung $R \hookrightarrow A$ einen $\text{Gal}(A, G)$ -Isomorphismus $A \otimes A \xrightarrow{\sim} A[G]^*$ an. Und zwar modifizieren wir Θ (vgl. 1.1.) zu

$$\Theta' : A \otimes A \ni a \otimes a' \mapsto \sum_g a g(a') d_g \in A[G]^* .$$

Θ' ist ein Isomorphismus von A -Algebren, aber auch mit der G -Struktur verträglich, also ein $\text{Gal}(A, G)$ -Iso-

morphismus, wie folgende Überlegung zeigt:

für $h \in G$ und $a, a' \in A$ ist

$$\begin{aligned} \Theta'(h(a \otimes a')) &= \Theta'(a \otimes h(a')) = \sum_g a \, g h(a') \, d_g = \\ &= \sum_g a \, g(a') \, d_{gh^{-1}} = h \left(\sum_g a \, g(a') \, d_g \right) = h \, \Theta'(a \otimes a'). \end{aligned}$$

Die andere Hälfte von (2.41.), die sich mit der o-ten Čechschen Kohomologie des Prägarbendiagrammes befaßt, ergibt sich als Folgerung aus (2.42.).

(2.42.) Proposition. R sei ein kommutativer Ring, G eine endliche abelsche Gruppe. Dann gilt:

Die Prägarben $U, \mu_2, V(-[G]), U(-[G])$ über der treuflachen Topologie sind Garben.

Beweis. Die Funktoren $U \simeq \underline{R\text{-Alg}}(R[\mathbb{Z}], -)$,

$\mu_2 \simeq \underline{R\text{-Alg}}(R[\mathbb{Z}/2\mathbb{Z}], -)$ sind darstellbar. Ist nun

$S \hookrightarrow T$ treuflach, so ist bekanntlich der additive Amitsurkomplex exakt $0 \longrightarrow S \longrightarrow T \rightrightarrows T \otimes_S T \longrightarrow \dots$.

Darstellbare Funktoren erhalten diesen Differenzkern, sie sind also Garben.

Wir zeigen anschließend in (2.43.), daß $V(-[G])$ durch die Hopf-Algebra $R[G]^*$ dargestellt wird. So bleibt also nur noch $U(-[G])$ zu betrachten.

$U(-[G])$ hat die Eigenschaft (+), denn : Ist $S \hookrightarrow T$

treuflach, so ist auch $S[G] \hookrightarrow T[G]$ treuflach ([29] S.11), insbesondere ist $U(S[G]) \longrightarrow U(T[G])$ injektiv.

Die assoziierte Garbe $U(-[G])^\#$ nimmt bei $S \in \underline{R\text{-Alg-tf}}$ folgenden Wert an

$$U(-[G])^\#(S) = \varinjlim_S \text{Ke}(U(T[G]) \rightrightarrows U(T \otimes_S T)[G])).$$

Die Komplexe

$$U(S[G]) \longrightarrow U(T[G]) \rightrightarrows U(T \otimes_S T)[G]) \dots$$

$$U(S[G]) \longrightarrow U(T[G]) \rightrightarrows U(T[G] \otimes_{S[G]} T[G]) \dots$$

sind isomorph, und da der untere Komplex für jede treuflache Erweiterung $S \hookrightarrow T$ exakt ist, ist $U(-[G])^\#(S) = U(S[G])$. Damit ist klar, daß $U(-[G]) = U(-[G])^\#$ eine Garbe ist.

(2.43.) Hilfssatz. Für $S \in \underline{R\text{-Alg}}$ ist die Zuordnung

$$\begin{aligned} \underline{R\text{-Alg}}(R[G]^*, S) &\longrightarrow V(S[G]) \\ f &\longmapsto \sum_g f(d_g) u_g \end{aligned}$$

ein Isomorphismus von Gruppen. Sie ist außerdem funktoriell in S .

Beweis. Ist $f : R[G]^* \longrightarrow S$ ein Algebrenhomomorphismus, so sind die $f(d_g), g \in G$ paarweise

orthogonale Idempotente, und ihre Summe ist 1. Also ist die Zuordnung wohldefiniert.

Sei andererseits ein System $(s_g)_{g \in G}$ von paarweise orthogonalen Idempotenten gegeben, deren Summe 1 ist. Durch $f(\sum_g r_g d_g) := \sum_g r_g s_g$ ist ein $f \in \underline{R}\text{-Mod}(\underline{R}[G]^*, S)$ bestimmt. Für dieses f ist $f(1) = f(\sum_g d_g) = \sum_g s_g = 1$, und es gilt

$$\begin{aligned} & f\left(\left(\sum_g r_g d_g\right)\left(\sum_h r'_h d_h\right)\right) \\ &= f\left(\sum_g r_g r'_g d_g\right) = \sum_g r_g r'_g s_g \\ &= \left(\sum_g r_g s_g\right)\left(\sum_h r'_h s_h\right) \\ &= f\left(\sum_g r_g d_g\right) f\left(\sum_h r'_h d_h\right). \end{aligned}$$

Also ist $f \in \underline{R}\text{-Alg}(\underline{R}[G]^*, S)$.

Die beiden Zuordnungen sind offenbar invers zueinander und funktoriell in S . Zu zeigen ist nur noch, daß sie die Gruppenstrukturen respektieren.

Seien $f, f' \in \underline{R}\text{-Alg}(\underline{R}[G]^*, S)$. Ihrem Produkt entspricht $\sum_g (f * f')(d_g) (u_g) =$

$$\begin{aligned} &= \sum_g \left(\sum_h f(d_h) f'(d_h^{-1}g) u_g \right) \\ &= \sum_g \sum_h f(d_h) f'(d_g) u_{hg}. \end{aligned}$$

Dies ist aber

gerade das Produkt der entsprechenden Elemente in $V(S[G])$.

Kapitel 3

DIE GRUPPE DER FREIEN QUADRATISCHEN ERWEITERUNGEN EINES RINGES, IN DEM 2 EIN NICHT-NULLTEILER IST

Das Ziel dieses Kapitels ist es, eine Methode zur Bestimmung der $\text{GF}(2)$ -Dimensionen der Gruppen $\mathcal{F}(R)$ zu finden.

In der Einleitung haben wir bereits ausführlich geschildert, wie sich die Lösung dieses Problems zusammen mit einer Reihe weiterer Resultate aus einem Diagramm exakter Kohomologiefolgen ergibt. In einem gewissen Sinn kulminieren die Ergebnisse der Kapitel 2, 3 und 4 in diesem Diagramm: nahezu Alles, was vor ihm kommt, dient seiner Herleitung, und fast alle späteren Resultate ergeben sich als Folgerungen aus ihm.

Doch der Weg zu diesem Gipfel ist leider noch mühsam und langwierig.

(3.0.) Bezeichnungen. In diesem Kapitel sei R ein kommutativer Ring, in welchem 2 ein Nicht-Nullteiler ist. Da wir hier nur quadratische Erweiterungen von R betrachten, verzichten wir bei den Invarianten auf die Indizes C_2 :

$\det_R := \det_R^{C_2}$, $\text{dis}_R := \text{dis}_R^{C_2}$, $\text{pic}_R := \text{pic}_R^{C_2}$. Die triviale quadratische Erweiterung sei $E_R := E_R^{C_2}$.

Desgleichen kommen nur Prägarben und Garben über der treuflachen Topologie $\overline{\mathcal{O}}_R$ vor (vgl. 2.40.), weshalb wir einfach von Prägarben bzw. Garben sprechen.

Daneben vereinbaren wir noch folgende Schreibweisen:

Für eine R-Algebra S sei

$$\varepsilon : S[C_2] \ni su_1 + s'u_t \longmapsto s + s' \in S$$

die Augmentation des Gruppenringes,

$$\pi_2 : S \ni s \longmapsto \bar{s} \in S/2S$$

$$\pi_4 : S \ni s \longmapsto \bar{\bar{s}} \in S/4S$$

$$\pi_2^4 : S/4S \ni \bar{\bar{s}} \longmapsto \bar{s} \in S/2S$$

seien die kanonischen Projektionen.

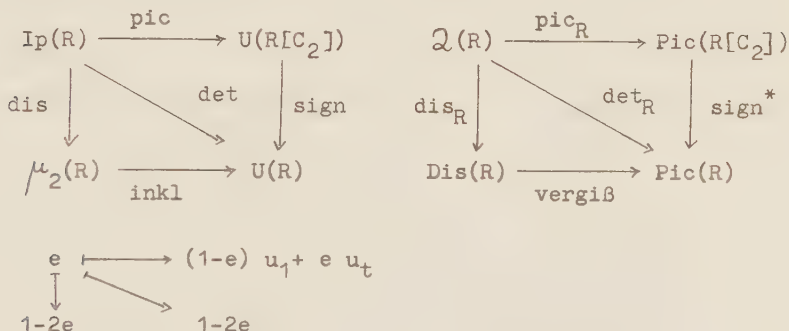
Daraus ergeben sich auf naheliegende Weise Morphismen von Prägarben $U\varepsilon, U\pi_2, U\pi_4, \mu_2\pi_2, \mu_2\pi_2^4$.

Für die Kern-Prägarben $\text{Ke}(U\pi_2)$ bzw. $\text{Ke}(U\pi_4)$ benutzen wir die Symbole U_2 bzw. U_4 .

An manchen Stellen ist es nötig, die Schreibweise noch mehr zu verkürzen, um gewisse Diagramme auf einer maschinengeschriebenen Seite darstellen zu können. Dort lassen wir Klammern und Indizes R weg, wenn aus dem Zusammenhang immer noch erkennbar ist, was gemeint ist (vgl. Einleitung).

§ 1 Das Invarianten-Diagramm im Fall quadratischer Erweiterungen

(3.1.) Für quadratische Erweiterungen nehmen die Diagramme der Invarianten und der Automorphismengruppen folgende Gestalt an (vgl. 2.20., 2.37.) :



(3.2.) Proposition. Ist 2 in R ein Nicht-Nullteiler, so sind $\text{det} : \text{Ip} \longrightarrow \text{U}$

$$\text{dis} : \text{Ip} \longrightarrow \mu_2$$

Monomorphismen in der Kategorie der Prägarben über der treuflachen Topologie.

Beweis. Es ist zu zeigen, daß für jede treuflache R-Algebra S die Abbildung $\text{Ip}(S) \ni e \longmapsto 1-2e \in \mu_2(S)$ injektiv ist. Man sieht dies aus den Äquivalenzen

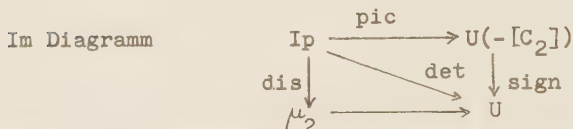
2 ist ein Nicht-Nullteiler in R

$$\iff \text{die Folge } 0 \longrightarrow R \xrightarrow{2} R \text{ ist exakt}$$

$$\iff \text{die Folge } 0 \longrightarrow S \xrightarrow{2} S \text{ ist exakt}$$

$$\iff 2 \text{ ist ein Nicht-Nullteiler in } S.$$

(3.3.) Bemerkung. Die Aussage von (3.2.) ist gerade das, was wir möchten : Den Homomorphismen aus (3.1.) sollen auf Prägarben-Niveau Monomorphismen entsprechen. Kokern-Prägarben ergänzen diese Monomorphismen zu kurzen exakten Folgen von Prägarben, und deren Čech-sche Kohomologiefolgen verbinden dann die jeweiligen Homomorphismen-Paare aus (3.1.).



sind nun bis auf sign alle Pfeile Monomorphismen. Wir erzwingen, daß auch an dieser Stelle ein Monomorphismus steht, indem wir $\text{U}(-[C_2])$ durch eine Unterprägarbe ersetzen, die zwar $\text{Bi}(\text{pic})$ enthält, aber mit $\text{Ke}(\text{sign})$ trivialen Durchschnitt hat.

(3.4.) Proposition. Sei $\text{Ke}(\text{U}\varepsilon)$ die Kern-Prägarbe zum Morphismus $\text{U}\varepsilon : \text{U}(-[C_2]) \longrightarrow \text{U}$. Da sie punktweise gebildet wird (2.40.3.), gilt für eine treuflache R-Algebra S

- a.) $\text{Bi}(\text{pic})(S) \subseteq \text{Ke}(\text{U}\varepsilon)(S)$
- b.) $\text{Ke}(\text{U}\varepsilon)(S) \cap \text{Ke}(\text{U sign})(S) = \{1\}$.

Beweis. a.) Für $e \in \text{Ip}(S)$ ist $\varepsilon \text{pic}(e) = \varepsilon((1-e)u_1 + eu_t) = 1$.

b.) Sei $su_1 + su_t \in \text{Ke}(\text{U}\varepsilon)(S) \cap \text{Ke}(\text{U sign})(S)$.

Dann ist $s + s' = 1 = s - s'$, also ist $2s = 2$. Da 2 ein Nicht-Nullteiler ist, folgt nun $s = 1$ und $s' = 0$.

(3.5.) Bemerkung. In (3.2.) sahen wir, daß die Bedingung "2 ist ein Nicht-Nullteiler in R" hinreichend dafür ist, daß $\det$ und dis Monomorphismen sind. Nun zeigt sich, daß sie notwendig ist, damit $\text{sign} : \text{Ke}(U\varepsilon) \longrightarrow U$ ein Monomorphismus von Prägarben ist.

Beweis. Sei $0 \neq r \in R$ mit $2r = 0$. Dann

$$\text{gelten } ((1-r)u_1 + ru_t)^2 = 1$$

$$(1-r) + r = 1$$

$$(1-r) - r = 1.$$

Also ist $1 \neq (1-r)u_1 + ru_t \in \text{Ke}(U \text{sign})(R) \cap \text{Ke}(U\varepsilon)(R)$.

(3.6.) Proposition. Der Prägarben-Morphismus

$\text{sign} : U(-[C_2]) \longrightarrow U$ induziert einen Isomorphismus von Prägarben $\text{Ke}(U\varepsilon) \xrightarrow{\sim} \text{Ke}(U\pi_2)$.

Beweis. Sei S eine treuflache R-Algebra. Für

$$su_1 + s'u_t \in \text{Ke}(U\varepsilon)(S) \text{ gilt}$$

$$(U\pi_2) \text{sign} (su_1 + s'u_t) = U\pi_2(s - s') =$$

$$= U\pi_2(1-2s') = \bar{1}.$$

Daher ist $\text{sign} : \text{Ke}(U\varepsilon)(S) \longrightarrow \text{Ke}(U\pi_2)(S)$ wohldefiniert. Die Injektivität sahen wir in (3.4.). Es bleibt also nur noch die Surjektivität zu zeigen.

Sei $u \in \text{Ke}(U\pi_2)(S)$. Dann gibt es $s, s' \in S$ mit $u = 1-2s$, $u^{-1} = 1-2s'$, und es gilt

$$\begin{aligned} & ((1-s)u_1 + su_t) ((1-s')u_1 + s'u_t) \\ &= (1-s-s' + 2ss')u_1 + (s + s' - 2ss')u_t = 1. \end{aligned}$$

Also ist $(1-s)u_1 + su_t \in \text{Ke}(U\varepsilon)(S)$ und $\text{sign}((1-s)u_1 + su_t) = u$.

Da $U(-[C_2])$ und U Garben sind (2.42.), ist auch $\text{Ke}(U\varepsilon)$ eine Garbe (2.40.4.). Also ist auch $U_2 := \text{Ke}(U\pi_2)$ (vgl. 3.0.) eine Garbe.

Das Prägarben-Diagramm aus Satz (2.41.) nimmt damit an der Stelle $S \in \underline{\text{R-Alg-tf}}$ folgende Gestalt an.

$$\begin{array}{ccc} \begin{array}{ccc} 0 & & 0 \\ \downarrow & & \downarrow \\ 0 \longrightarrow \text{Ip}(S) & \longrightarrow & U_2(S) \\ \downarrow & \searrow & \downarrow \text{inkl} \\ 0 \longrightarrow \mu_2(S) & \xrightarrow{\text{inkl}} & U(S) \end{array} & & \begin{array}{ccc} e & \xrightarrow{\quad} & 1 - 2e \\ \downarrow & \searrow & \\ 1 - 2e & & 1 - 2e \end{array} \end{array}$$

Bequemlichkeit halber bezeichnen wir auch diese Morphismen wieder als

$$\begin{array}{ccc} \begin{array}{ccc} 0 & & 0 \\ \downarrow & & \downarrow \\ 0 \longrightarrow \text{Ip} & \xrightarrow{\text{pic}} & U_2 \\ \downarrow \text{dis} & \searrow \text{det} & \downarrow \\ 0 \longrightarrow \mu_2 & \longrightarrow & U \end{array} & & \underline{(3.6.*)} \end{array}$$

(3.7.) Wir wollen nun überlegen, was der Übergang von $U(-[C_2])$ zu U_2 auf den ersten Čechschen Kohomologiegruppen bewirkt.

Die Struktur $\underline{G}$ aus (2.6.) hat für quadratische Erweiterungen die Pfeile $\nabla: 2 \rightarrow 1$, $\eta: 0 \rightarrow 1$, $t: 1 \rightarrow 1$, $1: 1 \rightarrow 1$. Die Struktur $\underline{P}$ zur Beschreibung von $\text{Pic}(R[C_2])$ ist die Teilstruktur $t: 1 \rightarrow 1$, $1: 1 \rightarrow 1$ von $\underline{G}$ (2.25.).

Für eine Galoiserweiterung $R \hookrightarrow A$ ist der Spur-morphismus $\text{tr}_R^A: A \rightarrow R$ (vgl. 1.2.) ein wichtiges Merkmal der Galois-Struktur. Man braucht ihn bei $\underline{G}$ nicht hinzuzunehmen, da er für $\underline{G}$ -Formen von E_R^G durch die übrigen Pfeile ausgedrückt werden kann. Wir erweitern $\underline{G}$ durch einen Pfeil $\text{tr}: 1 \rightarrow 0$ zu $\underline{G}'$. An den $\underline{G}$ -Formen von E_R^G ändert sich dadurch nichts.

Im quadratischen Fall betrachten wir nun die Unterstruktur $\underline{T}$ von $\underline{G}'$, deren Graph aus den Pfeilen $t, 1, \text{tr}$ besteht (vgl. 2.30.). Wir wollen nun $\check{H}^1(R, U_2)$ mit Hilfe von $\underline{T}$ -Formen der trivialen quadratischen Erweiterung E_R beschreiben.

Dazu machen wir uns klar, daß für eine R -Algebra S die Kategorie $\underline{T}_S$ (vgl. 2.5.2.) aus S -Moduln M zusammen mit S -Endomorphismen $t, 1: M \rightarrow M$ und einer Linearform $\text{tr}: M \rightarrow S$ besteht. Ihre Morphismen sind S -Modulhomomorphismen, welche mit $1, t, \text{tr}$ verträglich sind.

(3.8.) Satz. a.) Der Isomorphismus

$$\Gamma : \underline{P}_S\text{-aut}(E_S) \xrightarrow{\sim} U(S[C_2]) \quad (\text{vgl. 2.14., 2.25.})$$

induziert einen Isomorphismus auf den Untergruppen

$$\underline{T}_S\text{-aut}(E_S) \xrightarrow{\sim} \text{Ke}(U\varepsilon)(S), \quad S \in \underline{R}\text{-Alg.}$$

b.) Die in (2.31.) definierte Abbildung

$$V_{\underline{T}}^S(E_R) \longrightarrow V_{\underline{P}}^S(E_R), \quad S \in \underline{R}\text{-Alg-tf}$$

induziert einen injektiven Gruppenhomomorphismus

$$H^1(S/R, U_2) \longrightarrow \text{Pic}(R[C_2]).$$

c.) Durch Übergang zum Kolimes entsteht ein Isomorphismus abelscher Gruppen

$$\check{H}^1(R, U_2) \xrightarrow{\sim} \text{Ke}(\varepsilon^* : \text{Pic}(R[C_2]) \longrightarrow \text{Pic}(R)).$$

Beweis. a.) Seien S eine R -Algebra und f ein

$\underline{P}_S$ -Automorphismus von E_S mit $f(v_1) = sv_1 + s'v_t$. Γ ordnet f das Element $su_1 + s'u_t \in U(S[C_2])$ zu (vgl. 2.14.).

f ist genau dann ein $\underline{T}_S$ -Automorphismus, wenn folgendes Diagramm kommutiert

$$\begin{array}{ccc} E_S & \xrightarrow{\quad f \quad} & E_S \\ & \searrow \text{tr} & \swarrow \text{tr} \\ & S & \end{array}$$

Offensichtlich ist dies genau dann der Fall, wenn $s + s' = 1$ ist. Und das gilt wiederum genau dann, wenn $\Gamma(f) \in \text{Ke}(U\varepsilon)(S)$ ist.

b.) Sei nun S treuflach. Nach (2.16.) haben wir

dann eine Bijektion $V_{\underline{T}}^S(E_R) \simeq H^1(S/R, \text{Ke}(U\varepsilon))$.

Andererseits ist $H^1(S/R, \text{Ke}(U\varepsilon)) \longrightarrow H^1(S/R, U(-[C_2]))$

ein Homomorphismus abelscher Gruppen. Zusammen mit

den Isomorphismen $V_{\underline{P}}^S(E_R) \simeq \text{Pic}(S[C_2]/R[C_2]) \simeq$

$\simeq H^1(S/R, U(-[C_2]))$ aus (2.25.) und der Abbildung

$V_{\underline{T}}^S(E_R) \longrightarrow V_{\underline{P}}^S(E_R)$, gemäß (2.31.) bilden sie das

kommutative Diagramm

$$\begin{array}{ccc} V_{\underline{T}}^S(E_R) & \longrightarrow & V_{\underline{P}}^S(E_R) \simeq \text{Pic}(S[C_2]/R[C_2]) \\ \wr & & \wr \\ H^1(S/R, \text{Ke}(U\varepsilon)) & \longrightarrow & H^1(S/R, U(-[C_2])) \end{array} .$$

Wir wollen nun zeigen, daß die Abbildung

$V_{\underline{T}}^S(E_R) \longrightarrow V_{\underline{P}}^S(E_R)$ injektiv ist.

Sei $[M, 1, t, \text{tr}]$ eine $\underline{T}$ -Form von E_R bezüglich S

und $\beta: M \otimes S \xrightarrow{\sim} E_S$ ein $\underline{T}_S$ -Isomorphismus, dann

kommutiert folgendes Diagramm von S -Modulhomomorphismen

$$\begin{array}{ccc} M_S & \xrightarrow{\beta} & E_S \\ \downarrow t_S \quad \downarrow 1_S & & \downarrow t \quad \downarrow 1 \\ M_S & \xrightarrow{\beta} & E_S \\ \searrow \text{tr}_S & & \swarrow \text{tr} \\ & S & \end{array} .$$

Rechts steht ein Differenzkokern, also auch links. Da

S treuflach ist, ist bereits $M \xrightarrow[t]{t} M \xrightarrow{\text{tr}} R$ exakt.

Sei nun auch $[N, 1, t, tr]$ eine $\underline{T}$ -Form von E_R
 und $f : M \longrightarrow N$ ein $R[C_2]$ -Modulisomorphismus.
 Betrachten wir das Diagramm

$$\begin{array}{ccc}
 M & \xrightarrow[\sim]{f} & N \\
 \downarrow t \quad \downarrow 1 & & \downarrow t \quad \downarrow 1 \\
 M & \xrightarrow[\sim]{f} & N \\
 \downarrow tr & & \downarrow tr \\
 R & \xrightarrow[\sim]{h} & R
 \end{array}$$

Die Kokerneigenschaft beider Seiten zeigt, daß genau
 ein R -Modulisomorphismus h existiert, der das
 untere Viereck kommutativ macht. $a := h(1)$ ist
 invertierbar und $fa^{-1} : M \longrightarrow N$ ist ein $\underline{T}_R$ -Iso-
 morphismus.

$V_{\underline{T}}^S(E_R) \longrightarrow V_{\underline{P}}^S(E_R)$ ist also injektiv.

c.) Für einen Morphismus $S \longrightarrow S'$ treuflacher
 R -Algebren haben wir nun ein kommutatives Dreieck
 injektiver Gruppenhomomorphismen

$$\begin{array}{ccc}
 V_{\underline{T}}^S & & \\
 \downarrow \cong & \searrow & \\
 V_{\underline{T}}^{S'} & \searrow & \text{Pic}(R[C_2])
 \end{array}$$

Durch Übergang zum Kolimes ergibt sich also ein

injektiver Homomorphismus

$$\check{H}^1(R, \text{Ke}(U\xi)) =$$

$$= \varinjlim_R V_T^S = \bigcup_R V_T^S \hookrightarrow \text{Pic}(R[C_2]).$$

Ist M eine $\underline{T}$ -Form von E_R , so zeigt das Kokern-Diagramm $M \xrightarrow[1]{t} M \xrightarrow{\text{tr}} R$, daß $\varepsilon^*(M) = M \otimes_{R[C_2]} (\varepsilon R)$

$\simeq M/(1-t)M \simeq R$ isomorphe R -Moduln sind.

Sei nun $[M] \in \text{Pic}(R[C_2])$ und $\varepsilon^*(M) \simeq R$. tr sei die Komposition $M \longrightarrow M/(1-t)M \simeq \varepsilon^*(M) \simeq R$. Seien

außerdem $R \hookrightarrow S$ treuflach und $\beta: M_S \xrightarrow{\sim} E_S$ ein

$\underline{P}_S$ -Isomorphismus.

Wie vorher bilden wir das Diagramm

$$\begin{array}{ccc} M_S & \xrightarrow{\beta} & E_S \\ \downarrow t_S \quad \downarrow 1_S & & \downarrow t \quad \downarrow 1 \\ M_S & \xrightarrow{\beta} & E_S \\ \downarrow \text{tr}_S & & \downarrow \text{tr} \\ S & \xrightarrow{h} & S \end{array} .$$

Auf beiden Seiten stehen Kokerne, und das obere Viereck kommutiert in beiden Fällen. Deshalb gibt es genau einen S -Modulisomorphismus h , der das untere Viereck kommutativ macht. $a := h(1)$ ist invertierbar, und $\beta a^{-1}: M_S \longrightarrow E_S$ ist ein $\underline{T}_S$ -Isomorphismus. Also ist $[M]$ eine $\underline{T}$ -Form von E_R bezüglich S .

(3.9.) Zusammenfassung. Für die Invarianten quadratischer Erweiterungen eines Ringes R , in dem 2 ein Nicht-Nullteiler ist, haben wir ein kommutatives Diagramm von Prägarben mit exakten Zeilen und Spalten gefunden:

$$\begin{array}{ccccc}
 & 0 & & 0 & \\
 & \downarrow & & \downarrow & \\
 0 & \longrightarrow & \text{Ip} & \xrightarrow{\text{pic}} & \text{U}_2 \\
 & & \downarrow \text{dis} & \searrow \text{det} & \downarrow \text{inkl} \\
 0 & \longrightarrow & \mu_2 & \xrightarrow{\text{inkl}} & \text{U}
 \end{array}$$

Der 0-te Čechsche Kohomologie-Funktor $\check{H}^0(R, -)$ wertet es an der Stelle R aus :

$$\begin{array}{ccccc}
 & 0 & & 0 & \\
 & \downarrow & & \downarrow & \\
 0 & \longrightarrow & \text{Ip}(R) & \xrightarrow{\text{pic}} & \text{U}_2(R) \\
 & & \downarrow \text{dis} & \searrow \text{det} & \downarrow \\
 0 & \longrightarrow & \mu_2(R) & \longrightarrow & \text{U}(R)
 \end{array}$$

$\check{H}^1(R, -)$ macht daraus

$$\begin{array}{ccc}
 \mathcal{Q}(R) & \xrightarrow{\text{pic}_R} & \text{Ke}(\varepsilon^*) \\
 \downarrow \text{dis}_R & \searrow \text{det}_R & \downarrow \text{sign}^* \\
 \text{Dis}(R) & \xrightarrow{\text{vergiß}} & \text{Pic}(R)
 \end{array}$$

Die Besonderheit dieses Falles besteht darin, daß alle Morphismen des Prägarben-Diagrammes durch ihren Kokern zu einer kurzen exakten Folge ergänzt werden. Die beiden Diagramme der Automorphismen-gruppen und der Gruppen verzerrter Formen sind daher durch exakte Kohomologiefolgen verbunden (vgl. 2.40.).

In § 1 wollen wir noch die Kokern-Prägarben be-
stimmen. In der Kategorie $\mathcal{P}$ werden Kokerne punkt-
weise gebildet. Es genügt also, wenn wir sie für
eine treuflache R-Algebra S beschreiben.

(3.10.) Wir betrachten folgendes Diagramm abelscher
Gruppen

$$\begin{array}{ccccccc}
 & 0 & & 0 & & 0 & \\
 & \downarrow & & \downarrow & & \downarrow & \\
 0 & \longrightarrow & \text{Ip}(S) & \xrightarrow{\alpha'} & \text{U}_2(S) & \xrightarrow{\beta'} & \text{U}_2^2(S) \longrightarrow 0 \\
 & & \downarrow \vartheta' & & \downarrow \vartheta & & \downarrow \vartheta'' \\
 0 & \longrightarrow & \mu_2(S) & \xrightarrow{\alpha} & \text{U}(S) & \xrightarrow{\beta} & \text{U}^2(S) \longrightarrow 0 \\
 & & \downarrow \sigma' & & \downarrow \sigma & & \downarrow \sigma'' \\
 0 & \longrightarrow & \text{Bi}(\mu_2 \pi_2)(S) & \xrightarrow{\alpha''} & \text{Bi}(\text{U} \pi_2)(S) & \xrightarrow{\beta''} & \frac{\text{U}^2(S)}{\text{U}_2^2(S)} \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 0 & & 0 & & 0
 \end{array}$$

$$\begin{array}{ccccc}
 e & \xrightarrow{\quad} & 1-2e & u & \xrightarrow{\quad} & u^2 & v \\
 \downarrow & & & \downarrow & & & \downarrow \\
 1-2e & & & u & \xrightarrow{\quad} & u^2 & v \\
 \downarrow & & & \downarrow & & & \downarrow \\
 \bar{u} & \xrightarrow{\quad} & \bar{u} & \xrightarrow{\quad} & [u^2] & [v].
 \end{array}$$

(3.11.) Satz. Das Diagramm (3.10.) ist kommutativ und hat exakte Zeilen und Spalten. Alle auftretenden Morphismen sind funktoriell in S . Durch (3.10.) wird daher ein Diagramm von Prägarben beschrieben, welches kommutativ ist und exakte Zeilen und Spalten hat.

Beweis. Wir erinnern daran, daß stets $2 \in R$ als Nicht-Nullteiler vorausgesetzt ist.

Zunächst bemerken wir, daß β'' wohldefiniert ist — es ist die Faktorisierung von $\sigma''\beta$ über den Kokern von $\mathfrak{g}$.

Die Kommutativität ist klar, die Exaktheit der mittleren Zeile und der beiden rechten Spalten ebenfalls.

Zur linken Spalte: Offensichtlich ist $\text{Bi}(\mathfrak{g}') \subseteq \text{Ke}(\sigma')$. Sei nun $u \in \text{Ke}(\sigma')$. Dann gibt es ein $e \in S$, so daß $u = 1-2e$. $1 = u^2 = 1-4e + 4e^2$ zeigt, daß $e \in \text{Ip}(S)$ ist. Also ist $u \in \text{Bi}(\mathfrak{g}')$.

Zur oberen Zeile: Für $e \in \text{Ip}(S)$ ist $\beta'\alpha'(e) =$

$(1 - 2e)^2 = 1$. Also gilt: $\text{Bi}(\alpha') \subseteq \text{Ke}(\beta')$. Um die andere Inklusion zu zeigen, nehmen wir $u \in \text{Ke}(\beta')$. Dann ist $u^2 = 1$, und es gibt ein $e \in S$ mit $u = 1 - 2e$. Wie vorher folgt $e \in \text{Ip}(S)$. Daher ist $u \in \text{Bi}(\alpha')$.

Zur unteren Zeile: Ist $\bar{x} \in \text{Bi}(\alpha'')$, so gibt es ein $y \in S$ mit $y^2 = 1$ und $\bar{x} = \bar{y}$. Daher liegt $\bar{x}$ in $\text{Ke}(\beta'')$. Ist andererseits $\bar{y} \in \text{Ke}(\beta'')$, so ist $y \in U(S)$ und es gibt ein $x \in S$ mit $y^{-2} = (1-2x)^2$. Damit gilt $(y - 2xy)^2 = y^{-2} y^2 = 1$. Also ist $\bar{y} = \overline{y - 2xy} \in \text{Bi}(\mu_2 \pi_2)(S)$.

Wir wollen auch den Kokern von $\det : \text{Ip} \longrightarrow U$ beschreiben.

(3.12.) Proposition. Für eine treuflache R -Algebra S ist die Folge

$$0 \longrightarrow \text{Ip}(S) \xrightarrow{\det} U(S) \xrightarrow{\tau} U(S) \times U(S/2S) \\ e \longmapsto 1-2e \quad u \longmapsto (u^2, \bar{u})$$

exakt. Die beiden Morphismen sind funktoriell in S .

Beweis. Für $e \in \text{Ip}(S)$ ist $\tau \det(e) = ((1 - 2e)^2, \overline{1 - 2e}) = (1, \bar{1})$. Ist andererseits $u \in U(S)$ und $(u^2, \bar{u}) = (1, \bar{1})$, so gibt es ein $e \in S$ mit $u = 1 - 2e$. $1 = u^2 = 1 - 4e + 4e^2$ zeigt, daß $e^2 = e$ ist. Also ist $u \in \text{Bi}(\det)$.

§ 2 Die Gruppe der freien quadratischen Erweiterungen

(3.13.) Eine quadratische Erweiterung $R \hookrightarrow A$ ist als R -Modul treuprojektiv. Deshalb besitzt die Einbettung eine R -lineare Retraktion (vgl. [29] III.1.9.). In der direkten Summe $A = R \cdot 1 \oplus P$ ist P ein invertierbarer R -Modul, und es gilt $\bigwedge_R^2(A) \simeq P$. A ist also genau dann ein freier R -Modul, wenn $\det_R(A) \simeq R$ isomorph sind. Wir nennen A dann eine "freie quadratische Erweiterung".

Geht man zu den Isomorphieklassen über, so erkennt man, daß $\text{Ke}(\det_R)$ genau aus den Klassen freier quadratischer Erweiterungen besteht. Diese Untergruppe von $\mathcal{Q}(R)$ heißt "Gruppe der freien quadratischen Erweiterungen". Wir bezeichnen sie mit $\mathcal{F}(R)$ (vgl. Einleitung).

Wenn wir im folgenden auf Literatur über $\mathcal{F}(R)$ hinweisen, dann ist zu beachten:

Ist A eine separable R -Algebra, welche als R -Modul endlich erzeugt projektiv vom Rang 2 ist, so ist $R \rightarrow A$ injektiv, und es existiert genau ein Algebrenautomorphismus σ von A mit $\sigma^2 = \text{id}$ und $A^\sigma := \{a \in A \mid \sigma(a) = a\} = R$ ([38] §0). A ist also eine C_2 -Galoiserweiterung von R . Da der ausgezeichnete Automorphismus σ einer quadratischen Erweiterung

durch $\sigma^2 = \text{id}$ und $A^{\sigma} = R$ eindeutig bestimmt ist, überlegt man sich leicht, daß ein R -Algebrenisomorphismus zwischen quadratischen Erweiterungen bereits mit der Gruppenstruktur verträglich ist.

C. Small und Kitamura beschreiben $\mathcal{F}(R)$, indem sie Multiplikationen, welche den R -Modul $R \times R$ zu einer separablen R -Algebra machen, gewisse Tupel von Ringelementen zuordnen. Die Algebrenisomorphie induziert auf diesen Tupeln eine Äquivalenzrelation, und die Menge der Äquivalenzklassen entspricht dann $\mathcal{F}(R)$ (vgl. 3.17.).

Dagegen beschreiben wir nun $\mathcal{F}(R)$ auf die bereits in § 1 angedeutete Weise. Um die Schreibweise zu vereinfachen, bezeichnen wir die Bild-Prägarbe zum Morphismus $\mathcal{T}$, aus (3.12.), mit $W := \text{Bi}(\mathcal{T})$.

(3.14.) Satz. Die kurze exakte Folge von Prägarben

$$0 \longrightarrow \text{Ip} \xrightarrow{\det} U \xrightarrow{\mathcal{T}} W \longrightarrow 0 \quad (\text{vgl. 3.12.})$$

führt zur exakten Folge Čechscher Kohomologiegruppen

$$0 \longrightarrow \text{Ip}(R) \xrightarrow{\det} U(R) \xrightarrow{\mathcal{T}} \check{H}^0(R, W) \xrightarrow{F} \mathcal{Q}(R) \xrightarrow{\det_R} \text{Pic}(R) .$$

Dabei ist $\check{H}^0(R, W) = \{ (u, \bar{a}) \in U(R) \times U(R/2R) \mid u - a^2 \in 4R \}$

eine Untergruppe von $U(R) \times U(R/2R)$, und der "verbindende Homomorphismus" schickt $(u, \bar{a})$ mit $u - a^2 = 4b$, $b \in R$

auf die Klasse der quadratischen Erweiterung

$$R[x]/(x^2 - ax - b).$$

(3.15.) Folgerung. Durch die Isomorphie von $\mathcal{F}(R)$ mit dem Kokern von $\mathcal{T}: U(R) \longrightarrow \check{H}^0(R, W)$ erhält man folgende Beschreibung:

$\mathcal{F}(R) = \{ [u, \bar{a}] \mid (u, \bar{a}) \in U(R) \times U(R/2R), u - a^2 \in 4R \}$,
wobei $[u, \bar{a}] = \{ (v^2u, \overline{va}) \in U(R) \times U(R/2R) \mid v \in U(R) \}$;
 $[u_1, \bar{a}_1] [u_2, \bar{a}_2] = [u_1u_2, \overline{a_1a_2}]$ beschreibt die Verknüpfung, und $[1, \bar{1}]$ ist das neutrale Element.

Bevor wir nun Satz (3.14.) beweisen, stellen wir ein Hilfsmittel bereit.

(3.16.) Proposition. Seien $n \in R$ und $F: R\text{-Alg} \longrightarrow \underline{\text{Ab}}$ ein darstellbarer Funktor. Dann ist die Komposition $F(R/nR \otimes -)$ eine Garbe auf der treuflachen Topologie $\mathcal{T}_R$. Wir bezeichnen sie mit $F(-/n-)$.

Beweis von (3.16.). Sei $S \hookrightarrow T$ treuflach. Dann ist auch $S/nS \hookrightarrow T/nT$ treuflach (vgl. [29] S. 11).

Betrachten wir das Diagramm

$$\begin{array}{ccccc} S \otimes^R/nR & \longrightarrow & T \otimes^R/nR & \rightrightarrows & (T \otimes_S T) \otimes^R/nR \\ \wr & & \wr & & \wr \\ S/nS & \longrightarrow & T/nT & \rightrightarrows & T/nT \otimes_{S/nS} T/nT. \end{array}$$

Die kanonischen Isomorphismen machen es kommutativ. Da $S/nS \hookrightarrow T/nT$ treuflach ist, ist die untere Zeile exakt. Deshalb ist auch die obere Zeile exakt. F führt sie also in eine exakte Folge abelscher Gruppen über.

Beweis von Satz (3.14.). Da Produkte von Garben punktweise zu bilden sind, ist $U \times U(-/2-)$ eine Garbe (vgl. 2.40.). Ist $S \hookrightarrow T$ treuflach, so ist im kommutativen Diagramm

$$\begin{array}{ccccc} W(S) & \longrightarrow & W(T) & \xRightarrow{\quad} & W(T \otimes_S T) \\ \downarrow & & \downarrow & & \downarrow \\ U(S) \times U(S/2S) & \longrightarrow & U(T) \times U(T/2T) & \xRightarrow{\quad} & U(T \otimes_S T) \times U(T/2T \otimes_{S/2S} T/2T) \end{array}$$

die untere Zeile exakt. Deshalb ist $W(S) \longrightarrow W(T)$ injektiv. W hat also die Eigenschaft (+), und man kann $\check{H}^0(R, W) = W^{\#}(R)$ mit der Untergruppe $\bigcup_{\Omega_R} (W(S) \cap (U(R) \times U(R/2R)))$ von $U(R) \times U(R/2R)$ identifizieren (vgl. 2.40.).

Wir zeigen nun $\check{H}^0(R, W) =$

$$= \{ (u, \bar{a}) \in U(R) \times U(R/2R) \mid u - a^2 \in 4R \}.$$

" $\subseteq$ " : Seien $R \hookrightarrow S$ treuflach, $(u, \bar{a}) \in W(S) \cap (U(R) \times U(R/2R))$.

Dann gibt es also ein $v \in U(S)$ mit $u = v^2$, $\bar{a} = \bar{v}$. Sei $b \in S$ mit $v - a = 2b$. Man erkennt $u - a^2 = (v - a)(v + a) = 4b(b + a) \in 4S \cap R$. Es gilt aber $4S \cap R = 4R$, denn $R/4R \longrightarrow S/4S$ ist wieder treuflach, und folgendes Diagramm kommutiert

$$\begin{array}{ccccccc} 0 & \longrightarrow & 4R & \longrightarrow & R & \longrightarrow & R/4R \longrightarrow 0 \\ & & & & \downarrow & & \downarrow \\ 0 & \longrightarrow & 4S & \longrightarrow & S & \longrightarrow & S/4S \longrightarrow 0. \end{array}$$

" $\supseteq$ " : Sei nun $(u, \bar{a}) \in U(R) \times U(R/2R)$, und sei $b \in R$

mit $u - a^2 = 4b$. Die Erweiterung $R \hookrightarrow R[x]/(x^2 - ax - b)$ ist frei, also insbesondere treuflach. Für $v := a - 2x$ gilt $v^2 = a^2 - 4ax + 4x^2 = a^2 + 4b = u$. Also ist v invertierbar, und $\tau(v) = (v^2, \bar{v}) = (u, \bar{a})$ sind gleich.

Man überlegt sich leicht, daß $\check{H}^0(R, \tau)$ ein Element $v \in U(R)$ auf $(v^2, \bar{v}) = \tau(v) \in \check{H}^0(R, W)$ schickt.

Wenden wir uns also F zu. Seien $(u, \bar{a}) \in \check{H}^0(R, W)$ und $b \in R$ mit $u - a^2 = 4b$. Man macht sich schnell klar, daß durch die Vorschrift $\tilde{\sigma}(x) := a - x$ ein R -Algebrenautomorphismus von $S := R[x]/(x^2 - ax - b)$ bestimmt ist. Die Abbildung $R[x]/(x^2 - ax - b) \xrightarrow{q} E_S$,

$r_1 + r_2 x \mapsto (r_1 + r_2 x)v_1 + \tilde{\sigma}(r_1 + r_2 x)v_t$ ist also ein injektiver R -Algebrenhomomorphismus. Das Bild von q ist folgendermaßen charakterisiert:

$$\begin{aligned} &\forall s_1, s_2, t_1, t_2 \in R : \\ &(s_1 + s_2 x)v_1 + (t_1 + t_2 x)v_t \in \text{Bi}(q) \iff \\ &(t_1 = s_1 + as_2 \quad \text{und} \quad t_2 = -s_2). \end{aligned}$$

F ist der Kolimes der verbindenden Homomorphismen der Amitsurschen Kohomologiefolgen. Da $(u, \bar{a}) \in H^0(S/R, W)$ ist, für $S = R[x]/(x^2 - ax - b)$, genügt es folgendes Diagramm zu betrachten

$$\begin{array}{ccccccc}
 & & & & & 0 & \\
 & & & & & \downarrow & \\
 & & & & & W(S) \cap (U(R) \times U(R/2R)) & \\
 & & & & & \downarrow & \\
 \dots & & \dots & & \dots & & \\
 & \downarrow & & \downarrow & & & \\
 0 \longrightarrow & Ip(S) & \longrightarrow & U(S) & \xrightarrow{\tau} & W(S) & \longrightarrow 0 \\
 & \downarrow \downarrow & & \downarrow \downarrow & & \downarrow \downarrow & \\
 0 \longrightarrow & Z^1(S/R, Ip) & \longrightarrow & Z^1(S/R, U) & \xrightarrow{\tau} & Z^1(S/R, W) & \\
 & \downarrow & & \downarrow & & & \\
 & H^1(S/R, Ip) & & \dots & & & \\
 & \downarrow & & & & & \\
 & 0 & & & & & \\
 & & & & & (u, \bar{a}) & \\
 & & & & & \downarrow & \\
 & & & & & (v^2, \bar{v}) = (u, \bar{a}) & \\
 & & & & & \downarrow & \\
 & & & & & (1 \otimes 1, \overline{1 \otimes 1}) & \\
 e \longmapsto & (v \otimes 1)(1 \otimes v)^{-1} & \longmapsto & & & & .
 \end{array}$$

Wir bestimmen $e \in Ip(S \otimes S)$ mit $1 - 2e = v \otimes v^{-1}$.

Da $v^2 = u$, ist $v^{-1} = u^{-1}a - 2u^{-1}x$, und es gilt $v \otimes v^{-1} = 1 \otimes 1 - 2u^{-1}(2b(1 \otimes 1) + a(1 \otimes x) + a(x \otimes 1) - 2(x \otimes x))$.

Also ist e bestimmt. $F(u, \bar{a})$ gewinnt man nun durch

$$Ip(S \otimes S) \simeq V(S \otimes S[C_2]) \simeq \underline{\mathcal{Q}}(S \otimes S)\text{-aut}(E_{S \otimes S})$$

$$e \longmapsto (1-e)u_1 + eu_t \longmapsto g, \text{ mit}$$

$$g(v_1) = (1-e)v_1 + ev_t.$$

$F(u, \bar{a})$ ist die Klasse der bei g abgestiegenen quadratischen Erweiterung $A = \{sv_1 + s'v_t \in E_S \mid (s \otimes 1)v_1 + (s' \otimes 1)v_t = (1 \otimes s)g(v_1) + (1 \otimes s')g(v_t)\}$ (vgl. 2.16., 2.17.).

Seien $s_1, s_2, s'_1, s'_2 \in R$ und $s := s_1 + s_2 x$,

$s' := s'_1 + s'_2 x \in S$. Indem wir zunächst bei der $S \otimes S$ - Basis $\{v_1, v_t\}$ die Koeffizienten vergleichen und anschließend bei der R -Basis $\{1 \otimes 1, 1 \otimes x, x \otimes 1, x \otimes x\}$, ergeben sich folgende äquivalente Bedingungen

$$sv_1 + s'v_t \in A \iff \text{i.) } s \otimes 1 - 1 \otimes s = 1 \otimes (s' - s)e$$

$$\text{ii.) } 1 \otimes t - t \otimes 1 = 1 \otimes (s' - s)e$$

$$\iff \text{i.) } 0 = 2b(s'_1 - s_1) + ab(s'_2 - s_2)$$

$$\text{ii.) } -us_2 = a(s'_1 - s_1) + (a^2 + 2b)(s'_2 - s_2)$$

$$\text{iii.) } us_2 = a(s'_1 - s_1) - 2b(s'_2 - s_2)$$

$$\text{iv.) } 0 = -2(s'_1 - s_1) - a(s'_2 - s_2)$$

$$\text{v.) } us'_2 = -us_2$$

$$\iff (s'_2 = -s_2 \quad \text{und} \quad s'_1 = s_1 + as_2).$$

Wie wir uns schon vorher überlegt haben, ist

$A = \text{Bi}(q) \simeq R[x]/(x^2 - ax - b)$. Diese R -Algebra ist tatsächlich eine quadratische Erweiterung von R , denn sie repräsentiert eine verzerrte Form von E_R .

Wir wollen den Zusammenhang mit den bereits bekannten Beschreibungen aufzeigen.

(3.17.) Bemerkung. a.) C. Small [38] gibt für die Gruppe der freien quadratischen Erweiterungen folgende Beschreibung an:

$$\mathcal{Q}(R) = \{[u, a, r] \mid u \in U(R) ; a, r \in R; u a^2 + 4r = 1\};$$

$$[u, a, r] = [u', a', r'] \iff (\exists \alpha \in U(R), \beta \in R :)$$

$$\text{i.) } u' = \alpha^2 u$$

$$\text{ii.) } a' \alpha = a - 2\beta$$

$$\text{iii.) } r' = r + \beta(a - \beta) u ;$$

$$[u, a, r][u', a', r'] = [uu', aa', r + r' - 4rr'] ;$$

$[1, 1, 0]$ ist das neutrale Element ;

$$\mathcal{R}(R) \ni [u, a, r] \longmapsto \left[\frac{R[x, y]}{(1 - 2x - ay, x^2 - x + r, y^2 - u)} \right] \in \mathcal{Q}(R).$$

Bei dieser Beschreibung darf 2 auch ein Nullteiler sein.

b.) Aus den Ergebnissen von Kitamura [32] läßt sich eine entsprechende Beschreibung ableiten:

$$\mathcal{K}(R) = \{ [a, b] \mid a, b \in R, a^2 + 4b \in U(R) \} ;$$

$$[a, b] = [a', b'] \iff (\exists \alpha \in U(R), \beta \in R :$$

$$a' = \alpha(a - 2\beta)$$

$$b' = \alpha^2(\beta a + b - \beta^2) ;$$

$$[a, b][a', b'] = [aa', a^2b' + a'^2b + 4bb'] ;$$

$[1, 0]$ ist das neutrale Element;

$$\mathcal{K}(R) \ni [a, b] \longmapsto [R[x]/(x^2 - ax - b)] \in \mathcal{Q}(R).$$

Auch hier ist über 2 nichts vorauszusetzen.

(3.18.) Proposition. Nun sei 2 wieder ein Nicht-Nullteiler in R . Die drei Beschreibungen der Gruppe der freien quadratischen Erweiterungen sind durch folgende Isomorphismen miteinander verknüpft

$$\begin{array}{ccccc} \mathcal{R}(R) & \xrightarrow{\Psi} & \mathcal{K}(R) & \xrightarrow{\Upsilon} & \mathcal{F}(R) \\ [u, a, r] & \longmapsto & [a, ru^{-1}] & [a, b] \longmapsto & [a^2 + 4b, \bar{a}] \end{array} .$$

φ, ψ sind auch mit den Einbettungen in $\mathcal{Q}(R)$ verträglich.

Beweis. φ ist wohldefiniert:

$$\begin{aligned} [u, a, r] = [u', a', r'] &\implies (\exists \alpha \in U(R), \beta \in R : \\ a' &= \alpha^{-1}(a - 2\beta); r' u'^{-1} = (r + \beta(a - \beta)u) \alpha^{-2} u^{-1} = \\ \alpha^{-2}(\beta a + ru^{-1} - \beta^2)) &\implies [a, ru^{-1}] = [a', r' u'^{-1}]. \end{aligned}$$

$$\begin{aligned} \varphi \text{ ist ein Homomorphismus : } \varphi([u, a, r][u', a', r']) &= \\ = [aa', (r + r' - 4rr')u^{-1} u'^{-1}] &= [aa', a^2 r' u'^{-1} + a'^2 ru^{-1} + \\ 4rr' u^{-1} u'^{-1}] &= (\varphi[u, a, r])(\varphi[u', a', r']). \end{aligned}$$

$$\begin{aligned} \varphi \text{ ist injektiv : } [u, a, r] \in \text{Ke}(\varphi) &\implies [a, ru^{-1}] = [1, 0] \\ \implies (\exists \alpha \in U(R), \beta \in R : a &= \alpha(1 - 2\beta); ru^{-1} = \alpha^2(\beta - \beta^2)) \\ \implies (\exists \alpha \in U(R), \beta \in R : u^{-1} &= a^2 + 4ru^{-1} = \alpha^2; \\ a\alpha^{-1} = 1 - 2\beta; r &= \beta - \beta^2) \implies [u, a, r] = [1, 1, 0]. \end{aligned}$$

$$\begin{aligned} \varphi \text{ ist surjektiv : } [a, b] \in \mathcal{K}(R) &\implies \\ [(a^2 + 4b)^{-1}, a, b(a^2 + 4b)^{-1}] &\in \mathcal{K}(R) \text{ und} \\ \varphi[(a^2 + 4b)^{-1}, a, b(a^2 + 4b)^{-1}] &= [a, b]. \end{aligned}$$

$$\begin{aligned} \psi \text{ ist wohldefiniert : } [a, b] = [a', b'] &\implies (\exists \alpha \in U(R), \\ \beta \in R : a' &= \alpha(a - 2\beta), b' = \alpha^2(\beta a + b - \beta^2)) \implies \\ (\exists \alpha \in U(R) : a'^2 + 4b' &= \alpha^2(a^2 + 4b), \overline{a'} = \overline{\alpha a}) \\ \implies \psi[a, b] &= \psi[a', b']. \end{aligned}$$

$$\begin{aligned} \psi \text{ ist ein Homomorphismus : } \psi([a, b][a', b']) &= \\ = [a^2 a'^2 + 4a^2 b' + 4a'^2 b + 16bb', \overline{aa'}] &= \psi[a, b] \psi[a', b']. \end{aligned}$$

$$\begin{aligned} \psi \text{ ist injektiv : } [a^2 + 4b, \overline{a}] &= [1, \overline{1}] \implies (\exists \alpha \in U(R) : a^2 + 4b = \\ \alpha^2, \overline{a} = \overline{\alpha}) &\implies (\exists \alpha \in U(R), \beta \in R : \alpha^{-1}a = 1 - 2\beta, \\ 4\alpha^2(\beta - \beta^2) &= 4b) \implies [a, b] = [1, 0]. \end{aligned}$$

ψ ist surjektiv : $[u, \bar{a}] \in \mathcal{F}(R) \implies (\exists b \in R : u - a^2 = 4b)$
 $\implies (\exists b \in R : [a, b] \in \mathcal{K}(R), \psi[a, b] = [u, \bar{a}])$.

Es bleibt noch die Verträglichkeit mit den Einbettungen nach $\mathcal{Q}(R)$ zu zeigen. Für ψ stellt man fest, daß die beiden Vorschriften sogar identische Repräsentanten beschreiben.

Was φ anbelangt, so geben wir nun zueinander inverse R -Algebrenhomomorphismen zwischen den Repräsentanten an. Diese sind dann auch mit der C_2 -Struktur verträglich (vgl. 3.13.).

$$\frac{R[x, y]}{(1 - 2x - ay, x^2 - x + r, y^2 - u)} \xrightleftharpoons[\pi']{\pi} \frac{R[x]}{(x^2 - ax - ru^{-1})}$$

$$x \longmapsto 2r + uax$$

$$y \longmapsto ua - 2ux$$

$$ax - 2xu^{-1}y \longleftarrow x$$

π ist wohldefiniert : $1 - 2\pi(x) - a\pi(y) =$
 $= 1 - 4r - 2uax - ua^2 + 2aux = 0$ (vgl. 3.17.a.) ;
 $\pi(x)^2 - \pi(x) + r = 4r^2 + 4uarx + u^2a^2(ax + ru^{-1}) - 2r - uax + r$
 $= r(4r + ua^2) + uax(4r + ua^2) - r - uax = 0$;
 $\pi(y)^2 - u = u^2a^2 - 4u^2ax + 4u^2(ax + ru^{-1}) - u$
 $= u(ua^2 + 4r) - u = 0$.

π' ist wohldefiniert : $\pi'(x)^2 - a\pi'(x) - ru^{-1} =$
 $= a^2x^2 - 4aru^{-1}xy + 4r^2u^{-1}y^2 - a^2x + 2aru^{-1}y - ru^{-1}$
 $= a^2(x^2 - x) + 2aru^{-1}y(1 - 2x) - ru^{-1}(1 - 4r)$
 $= -a^2r + 2a^2ru^{-1}y^2 - ra^2 = 0$.

π und π' sind invers zueinander:

$$\pi\pi'(x) = \pi(ax - 2ru^{-1}y) = 2ra + ua^2x - 2ra + 4rx = x ;$$

$$\begin{aligned} \pi'\pi(x) &= \pi'(2r + uax) = 2r + ua^2x - 2ary = ua^2x + 2r(1-ay) = \\ &= (ua^2 + 4r)x = x ; \end{aligned}$$

$$\pi'\pi(y) = \pi'(ua - 2ux) = ua(1 - 2x) + 4ry = (ua^2 + 4r)y = y.$$

(3.19.) Quadratische Erweiterungen mit Normalbasis.

Eine Normalbasis für eine quadratische Erweiterung

$R \hookrightarrow A$ ist eine Basis der Form $\{a, t(a)\}$. Besitzt

A eine Normalbasis $\{a, t(a)\}$, so ist die Zuordnung

$R[C_2] \ni ru_1 + r'u_t \mapsto ra + r't(a) \in A$ ein Isomorphismus von $R[C_2]$ -Moduln. Umgekehrt ist durch einen

$R[C_2]$ -Isomorphismus $R[C_2] \xrightarrow{\sim} A$ eine Normalbasis von

A bestimmt. Die Isomorphieklassen quadratischer Er-

weiterungen mit Normalbasis bilden also genau die

Untergruppe $\text{Ke}(\text{pic}_R)$ von $\mathcal{Q}(R)$. Die Gruppe der

quadratischen Erweiterungen mit Normalbasis bezeich-

nen wir mit $\mathcal{N}(R)$.

Mit Hilfe der exakten Kohomologiefolge zur Picard-In-

variante können wir $\mathcal{N}(R)$ beschreiben.

(3.20.) Satz. Die obere Zeile von (3.10.) ist eine kurze exakte Folge von Prägarben. Die zugehörige lange exakte Folge Čechscher Kohomologiegruppen hat folgendes Anfangsstück

$$0 \longrightarrow \text{Ip}(R) \xrightarrow{\text{pic}} U_2(R) \xrightarrow{(\)^2} U_4(R) \xrightarrow{N} \mathcal{Q}(R) \xrightarrow{\text{pic}_R} \text{Ke}(\xi^*).$$

Dabei ist für $u \in U_4(R)$ mit $u = 1 + 4b$, $b \in R$ die Klasse $N(u) = [R[x]/(x^2 - x - b)]$.

Beweis. Nach (3.9.) ist nur noch der mittlere Teil der angegebenen Folge nachzuprüfen.

Zum Nachweis von $\check{H}^0(R, U_2^2) = U_4(R)$ überlegt man sich: $U(-/4-)$ ist eine Garbe (3.16.). Da Kerne in der Kategorie der Garben punktweise zu bilden sind, ist auch $U_4 = \text{Ke}(U \curvearrowright_4)$ eine Garbe. Es ist klar, daß $U_2^2(S) \hookrightarrow U_4(S)$ für jede R -Algebra S eine Untergruppe ist.

Ist nun $S \hookrightarrow T$ eine treuflache Erweiterung, so ist folgendes Diagramm kommutativ

$$\begin{array}{ccccc} U_2^2(S) & \longrightarrow & U_2^2(T) & \xRightarrow{\quad} & U_2^2(T \otimes_S T) \\ \downarrow & & \downarrow & & \downarrow \\ U_4(S) & \longrightarrow & U_4(T) & \xRightarrow{\quad} & U_4(T \otimes_S T) . \end{array}$$

Die untere Zeile ist exakt, also ist $U_2^2(S) \longrightarrow U_2^2(T)$ injektiv. U_2^2 hat daher die Eigenschaft (+). Man überlegt sich nun leicht, daß $\check{H}^0(R, U_2^2)$ bis auf Isomorphie mit folgender Vereinigung von Untergruppen in $U_4(R)$ übereinstimmt $\bigcup_{\Omega_R} U_4(R) \cap U_2^2(S)$ (vgl. 2.40.).

Es bleibt also zu zeigen, daß diese Vereinigung ganz $U_4(R)$ ergibt.

Sei dazu $u \in U_4(R)$. Dann gibt es ein $b \in R$ mit $u = 1 + 4b$. Sei $S := R[x]/(x^2 - x - b)$. S ist offensichtlich endlich erzeugt und treuflach. Es gilt $(1 - 2x)^2 = 1 - 4x + 4x^2 = 1 + 4b = u$. Also ist $1 - 2x \in U_2(S)$ und $u = (1 - 2x)^2 \in U_4(R) \cap U_2^2(S)$.

$\check{H}^0(R, \beta') : \check{H}^0(R, U_2) \longrightarrow \check{H}^0(R, U_2^2)$ ist der Kolimes über $[S] \in \Omega_R$ der auf den Differenzkernen induzierten Morphismen

$$\begin{array}{ccc}
 U_2(R) & \dashrightarrow & U_2^2(S) \cap U_4(R) \\
 \downarrow & & \downarrow \\
 U_2(S) & \xrightarrow{\beta'} & U_2^2(S) \\
 \begin{array}{c} d_1 \downarrow \\ \downarrow d_2 \end{array} & & \begin{array}{c} d_1 \downarrow \\ \downarrow d_2 \end{array} \\
 U_2(S \otimes S) & \xrightarrow{\beta'} & U_2^2(S \otimes S) .
 \end{array}$$

Man sieht, daß $\check{H}^0(R, \beta')$ durch $U_2(R) \ni u \mapsto u^2 \in U_4(R)$ beschrieben wird.

Wenn wir nun den "verbindenden Homomorphismus" N betrachten, so gehen wir wie im Beweis von Satz (3.14.) vor. Seien $u \in U_4(R)$, $b \in R$ mit $u = 1 + 4b$; $S := R[x]/(x^2 - x - b)$.

Wir betrachten folgendes Diagramm

$$\begin{array}{ccccccc}
 & \dots & & \dots & & U_2^2(S) \cap U_4(R) & \\
 & \downarrow & & \downarrow & & \downarrow & \\
 0 \longrightarrow & I_p(S) & \longrightarrow & U_2(S) & \xrightarrow{(\)^2} & U_2^2(S) & \longrightarrow 0 \\
 & \downarrow \downarrow & & \downarrow \downarrow & & \downarrow \downarrow & \\
 0 \longrightarrow & Z^1(S/R, I_p) & \longrightarrow & Z^1(S/R, U_2) & \longrightarrow & Z^1(S/R, U_2^2) & \\
 & \downarrow & & \downarrow & & \downarrow & \\
 & H^1(S/R, I_p) & & & & &
 \end{array}$$

$$\begin{array}{ccc}
 & & u \\
 & & \downarrow \\
 v = 1 - 2x & \mapsto & (1 - 2x)^2 = u \\
 \downarrow & & \downarrow \\
 e \longmapsto & (v \otimes 1)(1 \otimes v)^{-1} \mapsto & 1 \otimes 1
 \end{array}$$

In diesem Fall gilt $v \otimes v^{-1} = (1 - 2x) \otimes u^{-1}(1 - 2x) = 1 \otimes 1 - 2u^{-1}(2b(1 \otimes 1) + 1 \otimes x + x \otimes 1 - 2x \otimes x)$.
 e stimmt also mit dem Idempotent aus (3.14.) überein, wenn man dort $a = 1$ setzt. Die zugehörige verzerrte Form ist daher $[R[x]/(x^2 - x - b)]$.

(3.21.) Folgerung. Die Gruppe der quadratischen Erweiterungen mit Normalbasis ist isomorph zu $U_4(R)/U_2^2(R)$.
 Der Einbettung $\mathcal{N}(R) \hookrightarrow \mathcal{F}(R)$ entspricht der Homomorphismus

$$U_4(R)/U_2^2(R) \ni [u] \longmapsto [u, \bar{1}] \in \check{H}^0(R, W)/\text{Bi}(\tau) .$$

Er macht nämlich folgendes Diagramm kommutativ

$$\begin{array}{ccc} & \check{H}^0(R, W)/\text{Bi}(\tau) & \\ & \nearrow & \downarrow F \\ U_4(R)/U_2^2(R) & \xrightarrow{N} & \mathcal{Q}(R) . \end{array}$$

Beweis. Klar.

Bemerkung. Orzech [35] und Small [39] haben auf ganz andere Weise äquivalente Beschreibungen von $\mathcal{N}(R)$ gefunden.

(3.22.) Quadratische Erweiterungen mit trivialer Diskriminante. Während mehrere Arbeiten über die Kerne der Determinante und der Picard-Invariante existieren, scheint der Kern von $\text{dis}_R : \mathcal{Q}(R) \longrightarrow \text{Dis}(R)$ bisher vernachlässigt worden zu sein.

$\text{Ke}(\text{dis}_R)$ besteht aus den Isomorphieklassen quadratischer Erweiterungen $R \hookrightarrow A$, für welche $(\text{Ke}(\text{tr}_R^A), \text{mult}) \simeq (R, 1)$ isomorphe Diskriminantenmoduln sind. Dies läßt sich so ausdrücken: $\text{Ke}(\text{tr}_R^A)$ besitzt ein Basiselement aus $\mu_2(A)$.

Wir beschreiben die Gruppe der quadratischen Erweite-

ungen mit trivialer Diskriminante in der bereits vertrauten Weise.

(3.23.) Satz. Die Diskriminante ist Glied einer langen exakten Kohomologiefolge. Das Anfangsstück davon hat folgende Gestalt

$$0 \longrightarrow \text{Ip}(\mathbb{R}) \xrightarrow{\text{dis}} \mu_2(\mathbb{R}) \xrightarrow{\pi_2} \text{Bi}(\mu_2 \pi_2^4)(\mathbb{R}) \xrightarrow{T} \mathcal{Q}(\mathbb{R}) \xrightarrow{\text{dis}} {}^{\mathbb{R}}\text{Dis}(\mathbb{R}).$$

Dabei ist $\pi_2^4 : \mathbb{R}/4\mathbb{R} \longrightarrow \mathbb{R}/2\mathbb{R}$ die kanonische Projektion.

$\text{Bi}(\mu_2 \pi_2^4)(\mathbb{R})$ ist also eine Untergruppe von $\mu_2(\mathbb{R}/2\mathbb{R})$.

Ein Element daraus besitzt einen Repräsentanten $a \in \mathbb{R}$, so daß $a^2 - 1 = -4b$ ist, für ein $b \in \mathbb{R}$. $T(\bar{a})$ ist dann die Klasse der quadratischen Erweiterung $\mathbb{R}[x]/(x^2 - ax - b)$.

Beweis. Die zugehörige Folge von Prägarben ist

$$0 \longrightarrow \text{Ip} \longrightarrow \mu_2 \longrightarrow \text{Bi}(\mu_2 \pi_2) \longrightarrow 0 \quad (\text{vgl. 3.10.}).$$

$\mu_2(-/2-)$ ist eine Garbe (3.16.). Da

$$0 \longrightarrow \text{Bi}(\mu_2 \pi_2) \xrightarrow{\text{inkl}} \mu_2(-/2-) \text{ ein Monomorphismus von Prägarben ist, hat } \text{Bi}(\mu_2 \pi_2) \text{ die Eigenschaft (+), und es ist } \check{H}^0(\mathbb{R}, \text{Bi}(\mu_2 \pi_2)) = \bigcup_{\Omega_{\mathbb{R}}} \mu_2(\mathbb{R}/2\mathbb{R}) \cap \text{Bi}(\mu_2 \pi_2)(S).$$

Der Morphismus von $\mu_2(\mathbb{R})$ in diese Vereinigung von Untergruppen von $\mu_2(\mathbb{R}/2\mathbb{R})$ wird von π_2 induziert.

$$\text{Wir zeigen nun } \text{Bi}(\mu_2 \pi_2^4)(\mathbb{R}) = \bigcup_{\Omega_{\mathbb{R}}} \mu_2(\mathbb{R}/2\mathbb{R}) \cap \text{Bi}(\mu_2 \pi_2)(S).$$

" $\supseteq$ ": Seien $\mathbb{R} \hookrightarrow S$ treuflach und $\bar{a} \in \mu_2(\mathbb{R}/2\mathbb{R}) \cap \text{Bi}(\mu_2 \pi_2)(S)$, $a \in \mathbb{R}$. Dann gilt $a^2 - 1 \in 2\mathbb{R}$, und es gibt ein $b \in S$ mit

$b^2 = 1$ und $b - a \in 2S$. Sei $b - a = 2x$, $x \in S$.

Dann ist $a^2 = (b - 2x)^2 = 1 + 4(x^2 - bx)$, also liegt

$a^2 - 1$ in $4S \cap R = 4R$ (vgl. Beweis von 3.14.), und

es gilt: $\bar{a} \in \mu_2(R/4R)$ und $\pi_2^4(\bar{a}) = \bar{a}$.

" $\subseteq$ " Ein Element aus $\text{Bi}(\mu_2 \pi_2^4)(R)$ besitzt einen

Repräsentanten $a \in R$ mit $a^2 - 1 \in 4R$. Sei $a^2 - 1 =$

$-4b$, $b \in R$. Die R -Algebra $S := R[x]/(x^2 - ax - b)$

ist endlich erzeugt treuflach, und es gilt

$(2x - a)^2 = 4(x^2 - ax) + a^2 = 4b + (1 - 4b) = 1$.

Also liegt $\bar{a} = \overline{2x - a}$ in $\mu_2(R/2R) \cap \text{Bi}(\mu_2 \pi_2)(S)$.

Um zu sehen, wie der verbindende Homomorphismus T

operiert, nehmen wir a , b und S wie oben und

betrachten folgendes Diagramm

$$\begin{array}{ccccccc}
 & & & & \mu_2(R/2R) \cap \text{Bi}(\mu_2 \pi_2)(S) & & \\
 & & & & \downarrow & & \\
 0 & \longrightarrow & \text{Ip}(S) & \longrightarrow & \mu_2(S) & \longrightarrow & \text{Bi}(\mu_2 \pi_2)(S) \longrightarrow 0 \\
 & & \downarrow \downarrow & & \downarrow \downarrow & & \downarrow \downarrow \\
 0 & \longrightarrow & Z^1(S/R, \text{Ip}) & \longrightarrow & Z^1(S/R, \mu_2) & \longrightarrow & Z^1(S/R, \text{Bi}(\mu_2 \pi_2)) \\
 & & & & 2x - a \longmapsto \bar{a} = \overline{2x - a} & & \\
 & & & & \downarrow & & \\
 f & \longmapsto & (2x-a) \otimes (2x-a) = 1 \otimes 1 - 2[2b(1 \otimes 1) + a(1 \otimes x) + a(x \otimes 1) - 2(x \otimes x)] .
 \end{array}$$

Vergleicht man das Idempotent $e = 2b(1 \otimes 1) + a(1 \otimes x) +$

$a(x \otimes 1) - 2(x \otimes x)$ mit demjenigen aus dem Beweis von

(3.14.), so stellt man fest, daß hier der Spezialfall

$u = 1$ vorliegt. $T(\bar{a})$ ist die durch e bestimmte verzerrte Form: $T(\bar{a}) = [{}^R[x]/(x^2-ax-b)]$.

(3.24.) Folgerung. Die Gruppe der quadratischen Erweiterungen mit trivialer Diskriminante ist isomorph zu $\text{Bi}(\mu_2^4\pi_2)(R)/\text{Bi}(\mu_2\pi_2)(R)$.

Der Einbettung $\text{Ke}(\text{dis}_R) \hookrightarrow \mathcal{F}(R)$ entspricht der Homomorphismus

$$\text{Bi}(\mu_2^4\pi_2)(R)/\text{Bi}(\mu_2\pi_2)(R) \longrightarrow \check{H}^0(R,W)/\text{Bi}(\tau)$$

$$[\bar{a}] \longmapsto [1, \bar{a}] \quad .$$

Beweis. Klar.

§ 3 Das Diagramm der exakten Kohomologiefolgen

In (3.10.) haben wir ein kommutatives Diagramm von Prägarben beschrieben. Es besteht aus drei Zeilen und drei Spalten, welche jeweils kurze exakte Folgen sind. Wir wollen nun von allen Zeilen und Spalten Anfangsstücke der langen exakten Kohomologiefolgen bilden und diese dann endlich zum angekündigten großen Diagramm zusammenfügen.

Für die obere Zeile und die linke Spalte haben wir die Kohomologiefolge bereits in § 2 bestimmt. Die Folge zur mittleren Zeile findet man bei Micali und Villamayor [32].

(3.25.). Die exakte Folge der Čech'schen Kohomologiegruppen von $0 \longrightarrow \mu_2 \longrightarrow U \xrightarrow{()^2} U^2 \longrightarrow 0$ hat folgendes Anfangsstück (vgl. [32] 3.2.)

$$0 \longrightarrow \mu_2(R) \xrightarrow{\text{inkl}} U(R) \xrightarrow{()^2} U(R) \xrightarrow{\text{vergiß}} \text{Dis}(R) \xrightarrow{\text{vergiß}} \text{Pic}(R) .$$

$$u \longmapsto [R, h_u]$$

Dabei ist die Bilinearform h_u durch

$$R \otimes R \simeq R \ni 1 \longmapsto u \in R$$

bestimmt.

(3.26.) Proposition. Die Prägarbe $\text{Bi}(U\pi_2)$ hat die Eigenschaft (+), und es gilt :

$$\check{H}^0(R, \text{Bi}(U\pi_2)) = \bigcup_R U(R/2R) \cap \text{Bi}(U\pi_2)(S) = U(R/2R),$$

$$\check{H}^0(R, \mathfrak{G}) = U\pi_2(R) : U(R) \longrightarrow U(R/2R),$$

$$\check{H}^0(R, \alpha'') = \text{inkl} : \text{Bi}(\mu_2^4)(R) \longrightarrow U(R/2R).$$

($\mathfrak{G}$ und α'' sind wie in (3.10.).)

Beweis. $U(-/2-)$ ist eine Garbe (3.16.), und

$\text{Bi}(U\pi_2) \hookrightarrow U(-/2-)$ ist ein Monomorphismus von

Prägarben. Deshalb hat $\text{Bi}(U\pi_2)$ die Eigenschaft (+).

Ist S treuflach über R , so ist

$$U(R/2R) \cap \text{Bi}(U\pi_2)(S) = \text{Ke}(\text{Bi}(U\pi_2)(S) \xrightarrow[d_2]{d_1} \text{Bi}(U\pi_2)(S \otimes_R S)).$$

$\check{H}^0(R, \text{Bi}(U\pi_2))$ ist die Vereinigung dieser Untergruppen von $U(R/2R)$.

Wir zeigen nun: Ist $a \in R$ und $\bar{a} \in U(R/2R)$, so gibt es eine treuflache Erweiterung $R \hookrightarrow S$ und ein $u \in U(S)$ mit $\bar{u} = \bar{a}$. Sei $a \in R$ und $\bar{a} \in U(R/2R)$. Dann gibt es $x, y \in R$ mit $1 = ax + 2y$. $\{a, 2\}$ erzeugt also das Einheitsideal in R . Deshalb ist $S := R_a \times R_2$ eine treuflache R -Algebra ([29] S. 19). $R \ni r \mapsto (r, r) \in R_a \times R_2$ ist der Einismorphismus. Sei $u := a(1, 1) + 2(0, \frac{1-a}{2})$. Dann gilt $u(\frac{1}{a}, 1) = (a, a + 2 \frac{1-a}{2})$ $(\frac{1}{a}, 1) = (1, 1)$ und $u - a \in 2S$.

Um zu wissen, welcher Morphismus aus

$\mathcal{O} : U \longrightarrow \text{Bi}(U\pi_2)$ wird, genügt es

$H^0(S/R, \mathcal{O}) : H^0(S/R, U) \longrightarrow H^0(S/R, \text{Bi}(U\pi_2))$ für treuflache Erweiterungen $R \hookrightarrow S$ zu kennen. Dazu betrachten wir folgendes Diagramm

$$\begin{array}{ccccc} U(R) & \longrightarrow & U(S) & \xRightarrow{\quad} & U(S \otimes S) \\ \downarrow & & \mathcal{O} \downarrow & & \mathcal{O} \downarrow \\ U(R/2R) \cap \text{Bi}(U\pi_2)(S) & \longrightarrow & \text{Bi}(U\pi_2)(S) & \xRightarrow{\quad} & \text{Bi}(U\pi_2)(S \otimes S). \end{array}$$

Es ist kommutativ und hat exakte Zeilen. $H^0(S/R, \mathcal{O})$ ist die Einschränkung von $\mathcal{O}$ auf die Differenzkerne. Da $\mathcal{O}$ wiederum als Einschränkung von π_2 definiert ist, folgt die Behauptung.

Für eine treuflache R -Algebra S betrachten wir nun

$$H^0(S/R, \alpha'') : H^0(S/R, \text{Bi}(\mu_2 \pi_2)) \longrightarrow H^0(S/R, \text{Bi}(U\pi_2)).$$

Dies ist der Homomorphismus zwischen den Kernen im Diagramm

$$\begin{array}{ccccc} \text{Bi}(\mu_2 \pi_2)(S) \cap \mu_2(R/2R) & \longrightarrow & \text{Bi}(\mu_2 \pi_2)(S) & \xrightarrow{\quad} & \text{Bi}(\mu_2 \pi_2)(S \otimes S) \\ \downarrow & & \downarrow \alpha'' & & \downarrow \alpha'' \\ \text{Bi}(U\pi_2)(S) \cap U(R/2R) & \longrightarrow & \text{Bi}(U\pi_2)(S) & \xrightarrow{\quad} & \text{Bi}(U\pi_2)(S \otimes S). \end{array}$$

Man erkennt daraus, daß $H^0(S/R, \alpha'') = \text{inkl}$ ist.

Nun bleibt noch $\check{H}^0(R, U^2/U_2^2)$ zu bestimmen. Im Unterschied zu den anderen Fällen kommen wir dabei nicht damit aus, gewisse Untergruppen zu vereinigen.

(3.27.) Proposition.

a.) Für die Prägarbe U^2/U_2^2 sind $\check{H}^0(R, U^2/U_2^2) \simeq U(R/4R)$ isomorphe abelsche Gruppen.

b.) Identifizieren wir entlang diesem Isomorphismus, so gehen die Morphismen

$$\sigma'' : U^2 \longrightarrow U^2/U_2^2, \beta'' : \text{Bi}(U\pi_2) \longrightarrow U^2/U_2^2$$

(vgl. 3.10.) unter $\check{H}^0(R, -)$ in folgende Homomorphismen abelscher Gruppen über

$$U(R) \ni x \longmapsto \overline{x} \in U(R/4R), \quad U(R/2R) \ni \bar{x} \longmapsto \overline{\bar{x}^2} \in U(R/4R).$$

Beweis von (3.27.a.). Für eine treuflache R-Algebra S sei $K(S) := \text{Ke}(U^2(S)/U_2^2(S) \xrightarrow{\quad} U^2(S \otimes S)/U_2^2(S \otimes S))$.

Wir wollen zeigen, daß $\varinjlim_{\Omega_R} K(S) \simeq U(R/4R)$ isomorph sind.

Die kanonische Projektion π_4 induziert einen Homomorphismus $\frac{U^2(S)}{U_2^2(S)} \ni [u^2] \longmapsto \overline{u^2} \in U(S/4S)$. Er

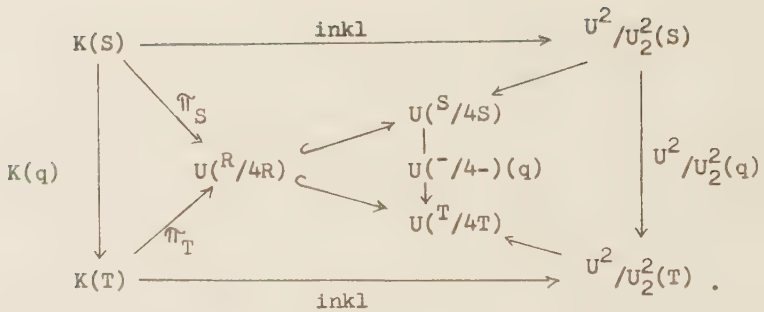
ist funktoriell in S , aber im allgemeinen nicht injektiv (vgl. 3.28.) Betrachten wir nun das Diagramm

$$\begin{array}{ccccccc} 0 & \longrightarrow & K(S) & \longrightarrow & U^2/U_2^2(S) & \rightrightarrows & U^2/U_2^2(S \otimes S) \\ & & \downarrow \pi_S & & \downarrow & & \downarrow \\ 0 & \longrightarrow & U(R/4R) & \longrightarrow & U(S/4S) & \rightrightarrows & U(S \otimes S/4(S \otimes S)) \end{array}$$

Da $U(-/4-)$ eine Garbe ist (3.16.), sind beide Zeilen exakt. Das rechte Viereck kommutiert für beide Pfeilpaare. Deshalb gibt es genau einen Pfeil π_S , der das linke Viereck kommutativ macht.

Um zu zeigen, daß die Familie $(\pi_S \mid [S] \in \Omega_R)$ mit den Morphismen der Indexkategorie Ω_R verträglich ist, wählen wir $[S] \leq [T]$ in Ω_R und einen R -Algebrenhomomorphismus $q : S \longrightarrow T$, der diese Relation induziert (vgl. 2.40.5.). Den von q induzierten Homomorphismus $K(S) \longrightarrow K(T)$ nennen wir $K(q)$.

Damit betrachten wir nun folgendes Diagramm



Von allen Teilen dieses Diagrammes außer dem linken Dreieck wissen wir bereits, daß sie kommutieren. Auch das äußere Viereck ist kommutativ. $\pi_T K(q)$ und π_S sind gleich, wenn man sie mit der injektiven Abbildung $U(R/4R) \longrightarrow U(T/4T)$ verknüpft. Deshalb gilt $\pi_T K(q) = \pi_S$.

Sei $\pi : \varinjlim K(S) \longrightarrow U(R/4R)$ der durch die Familie $(\pi_S \mid [S] \in \Omega_R)$ bestimmte Homomorphismus. In zwei Schritten zeigen wir, daß π ein Isomorphismus ist.

π ist injektiv : Sei $1 \in \varinjlim K(S)$ und $\pi(1) = \bar{1}$. Da Ω_R gerichtet ist, gibt es ein $[S] \in \Omega_R$ und $k \in K(S)$ mit $\pi_S(k) = \pi(1) = \bar{1}$. Um zu zeigen, daß 1 das neutrale Element ist, genügt es eine endlich erzeugte treuflache R -Algebra T und einen Morphismus $q : S \longrightarrow T$ anzugeben, so daß $K(q)(k)$ das neutrale Element in $K(T)$ ist.

Sei nun $u \in U(S)$ und $k = [u^2] \in U^2(S)/U_2^2(S)$. Wegen

$\overline{1} = \pi_S(k) = \overline{u^2}$ gibt es ein $b \in S$ mit $u^2 = 1+4b$.

Sei $T := S[x]/(x^2-x-b)$. $R \hookrightarrow S$ und $S \hookrightarrow T$

sind endlich erzeugte treuflache Erweiterungen,

also ist auch $R \hookrightarrow T$ endlich erzeugt und treu-

flach. Für q nehmen wir die Inklusion. $K(q)(k)$

ist dann die Klasse von u^2 in $U^2(T)/U_2^2(T)$. In T

gilt aber $(1-2x)^2 = 1 + 4(x^2 - x) = 1 + 4b = u^2$.

Also ist $u^2 \in U_2^2(T)$, $[u^2] = [1]$.

π ist surjektiv: Seien $a \in R$ und $\overline{a} \in U(R/4R)$.

Wie im Beweis von (3.26.) ist $S := R_a \times R_2$ eine

treuflache R -Algebra. Für $u := a(1, 1) + 4(0, \frac{1-a}{4}) \in U(S)$ ist

$u^{-1} = (\frac{1}{a}, 1)$, $u - a \in 4S$. In der Erweiterung

$R/4R \hookrightarrow S/4S$ gilt also $\overline{u} = \overline{a} \in U(R/4R)$.

Sei $T := \frac{S[x, y]}{(x^2 - 2x - (\frac{1-a}{a}, 0), y^2 - y - (0, \frac{a-1}{4}))}$.

Dann ist T eine endlich erzeugte treuflache Er-

weiterung von S , also auch von R . Für $v := (a, 1)(x-1)$

zeigen wir nun (i) $v \in U(T)$

(ii) $[v^2] \in K(T)$

(iii) $\pi_T[v^2] = \overline{a}$.

Es gilt: $v^2 = (a^2, 1)(x^2 - 2x - 1) = (a^2, 1)((\frac{1-a}{a}, 0) + (1, 1))$

$= (a^2, 1)(\frac{1}{a}, 1) = (a, 1) = u \in U(S)$. Also ist (i) erfüllt.

Für $[v^2] \in U^2(T)/U_2^2(T)$ ist $\overline{v^2} = \overline{u} = \overline{a}$. Wenn wir also

(ii) gezeigt haben, dann gilt auch (iii).

Sei $w := (0, \frac{1}{2}) \otimes x + (1, 0) \otimes y \in T \otimes T$. Dann ist

$$\begin{aligned} (1 \otimes 1 - 2w)^2 &= 1 \otimes 1 + 4(w^2 - w) \\ &= 1 \otimes 1 + 4 \left[(0, \frac{1}{4}) \otimes x^2 + (0, 0) \otimes xy + (1, 0) \otimes y^2 - (0, \frac{1}{2}) \otimes x - (1, 0) \otimes y \right] \\ &= 1 \otimes 1 + (0, 1) \otimes (x^2 - 2x) + (4, 0) \otimes (y^2 - y) \\ &= 1 \otimes 1 + (0, 1) \otimes (\frac{1-a}{a}, 0) + (4, 0) \otimes (0, \frac{a-1}{4}) \\ &= (0, 1) \otimes (1, 1) + (1, 0) \otimes (1, 1) + (0, 1) \otimes (\frac{1}{a} - 1, 0) + (1, 0) \otimes (0, a-1) \\ &= (0, 1) \otimes (\frac{1}{a}, 1) + (1, 0) \otimes (1, a) \\ &= (a, 1) \otimes (\frac{1}{a}, 1) = v^2 \otimes v^{-2} = (v^2 \otimes 1) (1 \otimes v^2)^{-1}. \end{aligned}$$

Deshalb ist $1 \otimes 1 - 2w \in U(T \otimes T)$ und

$(v^2 \otimes 1)(1 \otimes v^2)^{-1} \in U_2^2(T \otimes T)$. Damit ist (ii) gezeigt.

(3.28.) Beispiel. Wie wir bereits zu Beginn von (3.27.)

erwähnten, ist $\check{H}^0(R, U^2/U_2^2)$ i.a. nicht einfach die Vereinigung der $K(S)$. Dies präzisieren wir nun, indem wir für $R := \mathbb{Z}[\sqrt{5}]_{(\sqrt{5})}$ zeigen, daß $\pi_R : K(R) \rightarrow U(R/4R)$ nicht injektiv ist. Es ist nämlich $5 \in U^2(R) \cap U_4(R) = \text{Ke}(\pi_R)$, aber $5 \notin U_2^2(R)$, denn: $v \in U_2(S)$ und $v^2 = 5 \implies$

$1 + 2(a+b\sqrt{5})(\sqrt{5})^{-1} = v = \pm \sqrt{5}$; $a, b \in \mathbb{Z}$; $i \in \mathbb{N}_0 \implies$
 $2a + 2b\sqrt{5} = (\pm \sqrt{5} - 1)\sqrt{5}^i$. Vergleicht man die Koeffizienten der beiden Ausdrücke, so sieht man, daß dies nicht möglich ist.

Beweis von (3.27.b). $\check{H}^0(R, \sigma^n) : \check{H}^0(R, U^2) \rightarrow \check{H}^0(R, U^2/U_2^2)$

ist der Kolimes der Homomorphismen $H^0(S/R, \sigma'')$.

Für eine treuflache R-Algebra S kommutiert also folgendes Diagramm

$$\begin{array}{ccccccc}
 U(R) & \xleftarrow{\text{inkl}} & U(R) \cap U^2(S) & \longrightarrow & U^2(S) & \rightrightarrows & U^2(S \otimes S) \\
 \downarrow \check{H}^0(R, \sigma'') & & \downarrow u & & \downarrow \sigma'' & & \downarrow \sigma'' \\
 & \xleftarrow{\quad \bar{u} \quad} & [u] & & & & \\
 U(R/4R) & \xleftarrow{\pi_S} & K(S) & \longrightarrow & \frac{U^2(S)}{U^2_2(S)} & \rightrightarrows & \frac{U^2(S \otimes S)}{U^2_2(S \otimes S)}
 \end{array}$$

Für σ'' ist damit die Behauptung bewiesen.

Auf dieselbe Weise sieht man, was $\check{H}^0(R, \beta'')$ tut. Das entsprechende Diagramm ist

$$\begin{array}{ccccccc}
 U(R/2R) & \xleftarrow{\text{inkl}} & U(R/2R) \cap \text{Bi}(U\pi_2)(S) & \longrightarrow & \text{Bi}(U\pi_2)(S) & \rightrightarrows & \dots \\
 \downarrow \check{H}^0(R, \beta'') & & \downarrow & & \downarrow \beta'' & & \\
 U(R/4R) & \xleftarrow{\pi_S} & K(S) & \longrightarrow & \frac{U^2(S)}{U^2_2(S)} & \rightrightarrows & \dots
 \end{array}$$

Seien $x \in R$, $u \in U(S)$ und $\bar{x} = \bar{u}$ in $U(S/2S)$. Dann ist $\pi_S \beta''(\bar{x}) = \overline{u^2} = \overline{x^2}$.

Fassen wir nun unsere bisherigen Ergebnisse über die exakten Kohomologiefolgen der Zeilen und Spalten von (3.10.) zusammen.

(3.29.) Satz. Für einen kommutativen Ring R, in dem 2 ein Nicht-Nullteiler ist, ist folgendes Diagramm abelscher Gruppen kommutativ und hat exakte Zeilen und Spalten

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & \text{Ip}(R) & \longrightarrow & U_2(R) & \longrightarrow & U_4(R) \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & \mu_2(R) & \longrightarrow & U(R) & \longrightarrow & U(R) \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & \text{Bi}\mu_2\pi_2^4(R) & \longrightarrow & U^{(R/2R)} & \longrightarrow & U^{(R/4R)} \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & \text{Ip}(R) & \longrightarrow & U_2(R) & \longrightarrow & U_4(R) \longrightarrow Q(R) \xrightarrow{\text{pic}_R} \text{Ke}(\xi^*) \\
 & & \downarrow & & \downarrow & & \downarrow \text{dis}_R \searrow \text{det}_R \downarrow \text{sign}^* \\
 0 & \longrightarrow & \mu_2(R) & \longrightarrow & U(R) & \longrightarrow & U(R) \longrightarrow \text{Dis}(R) \longrightarrow \text{Pic}(R) \\
 & & \downarrow & & \downarrow & & \downarrow \text{vergi\ss} \\
 0 & \longrightarrow & \text{Bi}\mu_2\pi_2^4(R) & \longrightarrow & U^{(R/2R)} & \longrightarrow & U^{(R/4R)}
 \end{array}$$

$$\begin{array}{ccccc}
 e & \mapsto & 1-2e & a & \mapsto & a^2 & u \\
 \downarrow & & \downarrow & \downarrow & & \downarrow & \downarrow \\
 1-2e & & a & \mapsto & a & \mapsto & a^2 & u \\
 \downarrow & & \downarrow & \downarrow & & \downarrow & \downarrow \\
 \bar{a} & \mapsto & \bar{a} & \mapsto & \bar{a} & \mapsto & \bar{a}^2 & \bar{u} \\
 \downarrow & & \downarrow & & & & \downarrow \\
 & & F[1, \bar{a}] & & & &
 \end{array}$$

$$\begin{array}{ccccccc}
 e & \mapsto & 1-2e & a & \mapsto & a^2 & u & \mapsto & F[u, \bar{1}] & [A] & \longrightarrow & [A] \\
 \downarrow & & \downarrow & \downarrow & & \downarrow & \downarrow & & \downarrow & \swarrow & & \\
 1-2e & & a & \mapsto & a & \mapsto & a^2 & u & \mapsto & [R, h_u] & [\text{Ketr}, \text{mult}] & [\text{Ketr}] \\
 \downarrow & & \downarrow & \downarrow & & \downarrow & \downarrow & & \downarrow & & & \\
 \bar{a} & \mapsto & \bar{a} & \mapsto & \bar{a} & \mapsto & \bar{a}^2 & \bar{u} & & & &
 \end{array}$$

§ 4 Diskriminanten und Picard-Invarianten freier quadratischer Erweiterungen

In diesem Paragraphen werden wir mit Hilfe des Diagrammes der exakten Kohomologiefolgen die Gruppe $\mathcal{F}(R)$ untersuchen. R ist dabei — wie generell in Kapitel 3 — ein kommutativer Ring, in welchem 2 ein Nicht-Nullteiler ist.

(3.30.). Kitamura [28] definierte einen Homomorphismus D von der Gruppe der freien quadratischen Erweiterungen in die Quadratklassengruppe $U(R)/U^2(R)$.

D ordnet der Klasse der Erweiterung $R[x]/(x^2-ax-b)$, $a^2 + 4b \in U(R)$ das Element $[a^2 + 4b] \in U(R)/U^2(R)$ zu. Mit den Bezeichnungen von (3.17.) wird aus D folgende Zuordnung

$$\begin{aligned} \mathcal{F}(R) &\xrightarrow{\sim} \mathcal{K}(R) \longrightarrow U(R)/U^2(R) \\ [u, \bar{a}] &\longmapsto [a, b] \longmapsto [a^2 + 4b] = [u] \quad . \\ u - a^2 &= 4b \end{aligned}$$

Wenn man sich anschaut, wie $\mathcal{F}(R) = \check{H}^0(R, W)/\text{Bi}(\tau)$ gebildet ist (3.15.), dann erkennt man auch direkt, daß diese Zuordnung wohldefiniert und ein Homomorphismus ist. Wir bezeichnen sie ebenfalls mit D .

(3.31.) Satz. Identifiziert man $U(R)/U^2(R)$ mit der Gruppe der freien Diskriminantenmoduln, so stimmt $D : \mathcal{F}(R) \longrightarrow U(R)/U^2(R)$ mit der Einschränkung der Diskriminante $\mathcal{Q}(R) \longrightarrow \text{Dis}(R)$ überein, d.h. folgendes Diagramm kommutiert

$$\begin{array}{ccc} \mathcal{F}(R) & \xrightarrow{F} & \mathcal{Q}(R) \\ D \downarrow & & \downarrow \text{dis}_R \\ U(R)/U^2(R) & \xrightarrow{\quad} & \text{Dis}(R) . \end{array}$$

Bezeichnung. Wir nennen D die "Diskriminante der freien quadratischen Erweiterungen von R ".

Beweis. $U(R)/U^2(R) \ni [u] \longmapsto [R, h_u] \in \text{Dis}(R)$ ist der Kern von $\text{vergiß} : \text{Dis}(R) \longrightarrow \text{Pic}(R)$ (3.25.). Man kann deshalb $U(R)/U^2(R)$ als die Gruppe der freien Diskriminantenmoduln auffassen.

Sei nun $[u, \bar{a}] \in \mathcal{F}(R)$, für $b \in R$ sei $u - a^2 = 4b$. Dann ist $F[u, \bar{a}] = [R[x]/(x^2 - ax - b)]$ (vgl. 3.14.). Wie wir in (3.13.) erwähnten, ist die C_2 -Struktur einer quadratischen Erweiterung eindeutig bestimmt. Der nicht-triviale Automorphismus $\mathcal{G}$ ist im Fall der Erweiterung $S := R[x]/(x^2 - ax - b)$ durch die Vorschrift $\mathcal{G}(x) := a - x$ bestimmt. Wir deuten kurz an, wie man die einzelnen Eigenschaften verifiziert.

$\mathcal{G}$ ist wohldefiniert : $\mathcal{G}(x^2 - ax - b) = (a - x)^2 - a(a - x) - b = x^2 - ax - b = 0$.
 $\mathcal{G}^2 = \text{id} : \mathcal{G}(a - x) = a - (a - x) = x$;
 $S^{\mathcal{G}} = R : r_1 + r_2 x = \mathcal{G}(r_1 + r_2 x) = r_1 + r_2 a - r_2 x \implies$
 $r_1 + r_2 a = r_1 \quad \text{und} \quad -r_2 = r_2 \implies r_2 = 0$.

Für den Spurhomomorphismus $R[x]/(x^2 - ax - b) \xrightarrow{\text{tr}_R^S} R$

gilt also $\text{tr}_R^S(1) = 2$, $\text{tr}_R^S(x) = a$. $\text{Ke}(\text{tr}_R^S)$ ist ein freier R -Modul (vgl. 3.9.), und $(\text{Ke}(\text{tr}_R^S), \text{mult})$ ist ein Diskriminantenmodul (vgl. 1.25.). Es gibt deshalb ein Basiselement $s \in \text{Ke}(\text{tr}_R^S)$ mit $\text{Ke}(\text{tr}_R^S) = R \cdot s$ und $s^2 \in U(R)$. Sei $s = \alpha 1 + \beta x$ mit $\alpha, \beta \in R$.

Dann gilt : $0 = \text{tr}_R^S(\alpha + \beta x) = 2\alpha + \beta a$;

$s^2 = \alpha^2 + (2\alpha + \beta a)\beta x + \beta^2 b = \alpha^2 + \beta^2 b \in U(R)$;

$u(\alpha^2 + \beta^2 b) = (a^2 + 4b)(\alpha^2 + \beta^2 b) = (\alpha a - 2\beta b)^2$.

Deshalb ist $(\alpha a - 2\beta b)(\alpha^2 + \beta^2 b)^{-1} \in U(R)$,

$z := (\alpha a - 2\beta b)(\alpha^2 + \beta^2 b)^{-1}s$ ist ebenfalls ein

Basiselement für $\text{Ke}(\text{tr}_R^S)$, und es gilt $z^2 = u$. Also

ist $f : R \longrightarrow \text{Ke}(\text{tr}_R^S)$, $f(1) := z$ ein Isomorphismus von Diskriminantenmoduln $(R, h_u) \xrightarrow{\sim} (\text{Ke}(\text{tr}_R^S), \text{mult})$.

Also entspricht $D[u, \bar{a}]$ folgender Klasse von Dis-

kriminantenmoduln $[R, h_u] = [\text{Ke}(\text{tr}_R^S), \text{mult}] = \text{dis}_R F[u, \bar{a}]$

(vgl. 1.25.c).

(3.32.) Bemerkungen. a.) Auch Kitamura erhielt den

Homomorphismus $D : \mathcal{F}(R) \longrightarrow U(R)/U^2(R)$ als

Einschränkung eines auf ganz $\mathcal{Q}(R)$ definierten Homo-

morphismus. Und zwar handelte es sich dabei um einen

von Kanzaki [27] betrachteten Morphismus

$\mathcal{Q}(R) \longrightarrow U(W^*(R))$ in die Einheitengruppe des

verallgemeinerten Witttringes.

b.) Das Diagramm aus (3.31.) kommutiert auch dann,

wenn 2 ein Nullteiler ist. In diesem Fall ist allerdings statt $\mathcal{F}(R)$ die Gruppe $\mathcal{K}(R)$ zu nehmen.

Wie schon in der Einleitung erwähnt wurde, hat Thérond [41] die Gruppen $\mathcal{F}$ für Hauptordnungen in quadratischen Zahlkörpern bestimmt, indem er $\text{Ke}(D)$ und $\text{Bi}(D)$ untersuchte.

Diesen Gedanken wollen wir nun aufgreifen.

An allgemeinen Ergebnissen über $\text{Ke}(D)$ gab es bisher nur einige hinreichende Bedingungen dafür, daß D ein Monomorphismus ist (vgl. Kitamura [28]). Doch diese erwiesen sich bereits für die von Thérond betrachteten Ringe als unzureichend.

Unser Hauptergebnis über die Gruppen der freien quadratischen Erweiterungen wird eine exakte 7-Term-Folge sein, in deren Mitte D steht. Ihr kann man Beschreibungen von $\text{Ke}(D)$ und $\text{Bi}(D)$ entnehmen.

(3.33.) Satz. Die "Diskriminanten-Spalte" des Diagrammes (3.29.) ergibt eine sieben-gliedrige exakte Folge, in deren Mitte die Diskriminante der freien quadratischen Erweiterungen steht.

$$\begin{array}{c}
 e \\
 \downarrow \\
 1-2e \\
 a \\
 \downarrow \\
 \bar{a} \\
 \downarrow \\
 [1, \bar{a}] \\
 [u, \bar{a}] \\
 \downarrow \\
 [u] \\
 \downarrow \\
 [\bar{u}] \\
 \downarrow \\
 [\bar{\bar{u}}]
 \end{array}
 \qquad
 \begin{array}{c}
 0 \\
 \downarrow \\
 Ip(R) \\
 \downarrow \\
 \mu_2(R) \\
 \downarrow \\
 Bi(\mu_2^4)(R) \\
 \downarrow \\
 \mathcal{F}(R) \\
 \downarrow \quad D \\
 \frac{U(R)}{U^2(R)} \\
 \downarrow \\
 \frac{U(R/4R)}{U^2(R/4R)} \\
 \downarrow \\
 \frac{U(R/4R)}{U^2(R/4R) + Bi(U\pi_4)(R)} \\
 \downarrow \\
 0
 \end{array}$$

(Obwohl wir unsere Gruppen — auch die abelschen — im allgemeinen multiplikativ schreiben, haben wir beim letzten Glied der Folge die Summe zweier Untergruppen durch " + " ausgedrückt.)

(3.34.) Folgerungen. Sei 2 in R ein Nicht-Nullteiler.

a.) $\text{Ke}(D) \simeq \frac{\text{Bi}(\mu_2^4 \pi_2)(R)}{\text{Bi}(\mu_2 \pi_2)(R)}$ sind isomorphe abelsche

Gruppen.

b.) Folgendes Kriterium ist hinreichend dafür, daß

D injektiv ist:

$$\forall a \in R [a^2 - 1 \in 4R \implies a - 1 \in 2R].$$

c.) Ist R ein Integritätsring mit einer von 2 verschiedenen Charakteristik, so sind

$\text{Ke}(D) \simeq \text{Bi}(\mu_2^4 \pi_2)(R)$ isomorph. Das Kriterium aus b.) ist in diesem Fall auch notwendig für die Injektivität von D.

Beweis von (3.34.). a.) folgt aus (3.33.).

b.) Das Kriterium besagt genau, daß $\text{Bi}(\mu_2^4 \pi_2)(R)$ einpunktig ist. Ist es erfüllt, so ist also $\text{Ke}(D)$ trivial.

c.) Ist R ein Integritätsring, so ist $\mu_2(R) = \{\pm 1\}$. Die Behauptung ergibt sich daraus mit Hilfe von a.) und der Überlegung im Beweis von Teil b.).

Das Kriterium (3.34.b.) und die gewonnene Beschreibung von $\text{Ke}(D)$ werden sich in Kapitel 4 als brauchbare Hilfsmittel erweisen, um für Ordnungen in quadratischen Zahlkörpern die Gruppe $\mathcal{F}$ zu bestimmen.

(3.35.) Folgerung. Sei 2 in R ein Nicht-Nullteiler. Aus (3.33.) und (3.34.b.) erhält man Kitamuras Ergebnisse ([28] Theorem 4) :

- a.) Ist R ein ZPE-Ring der Charakteristik $\neq 2$, so ist D injektiv.
- b.) Ist 2R ein Primideal von R, so ist D injektiv.
- c.) Ist 2 in R invertierbar, so ist D ein Isomorphismus.

Beweis von (3.33.). Um zu sehen, wie die angegebene Folge aus der vierten Spalte von (3.29.) entsteht, betrachten wir folgendes Diagramm

$$\begin{array}{ccc}
 & & \begin{array}{c} 0 \\ \downarrow \\ \text{Ip}(R) \\ \downarrow \\ \mu_2(R) \\ \downarrow \\ \text{Bi}(\mu_2 \pi_2^4)(R) \end{array} \\
 & \swarrow F & \downarrow T \\
 \mathcal{F}(R) & \hookrightarrow & \mathcal{Q}(R) \\
 D \downarrow & & \downarrow \text{dis}_R \\
 \frac{U(R)}{U^2(R)} & \hookrightarrow & \text{Dis}(R) \\
 \downarrow & & \downarrow \\
 \frac{U(R/4R)}{U^2(R/4R)} & \hookrightarrow & H^1(R, \text{Bi}(\mu_2 \pi_2^4)) \\
 \downarrow & & \\
 \frac{U(R/4R)}{U^2(R/4R) + \text{Bi}(U\pi_4)(R)} & & \\
 \downarrow & & \\
 0 & & .
 \end{array}$$

Die ersten beiden Pfeile bleiben ungeändert. Die erste Änderung kommt dadurch zustande, daß wir T über $\mathcal{F}(R)$ faktorisieren. Dabei benutzen wir (3.24.). Da F injektiv ist, ist auch die modifizierte Folge bei $Bi(\mu_2^4\pi_2^4)(R)$ exakt.

Als nächstes ersetzen wir dis_R durch die Diskriminante der freien quadratischen Erweiterungen. Die Exaktheit der neuen Folge bei $\mathcal{F}(R)$ ergibt sich mit Hilfe von (3.31.) aus der Exaktheit der alten Folge bei $\mathcal{Q}(R)$.

Beim fünften Term haben wir $Dis(R)$ durch den Kern von $Dis(R) \xrightarrow{\text{vergiß}} Pic(R)$ bzw. den Kokern von $U(R) \xrightarrow{(\)^2} U(R)$ ersetzt. Beim nächsten Term gehen wir genauso vor und setzen an die Stelle von $\check{H}^1(R, Bi(\mu_2^4\pi_2^4))$ den Kokern von $U(R/2R) \ni \bar{a} \longmapsto \overline{a^2} \in U(R/4R)$. Als fünften Pfeil wählen wir den durch $U\mathcal{U}_4$ auf den Kokernen induzierten Homomorphismus.

Um den gewünschten Kokern angeben zu können, zeigen wir nun, daß $U^2(R/4R)$ mit dem Bild des betrachteten Homomorphismus übereinstimmt. Daß $U^2(R/4R)$ im Bild liegt, ist klar. Für den Nachweis der umgekehrten Inklusion sei $a \in R$ mit $\bar{a} \in U(R/2R)$.

Es gibt dann ein $b \in R$, für welches $ab - 1 \in 2R$ ist. Dafür ist $a^2b^2 - 1 = (ab - 1)(ab + 1) \in 4R$, also ist

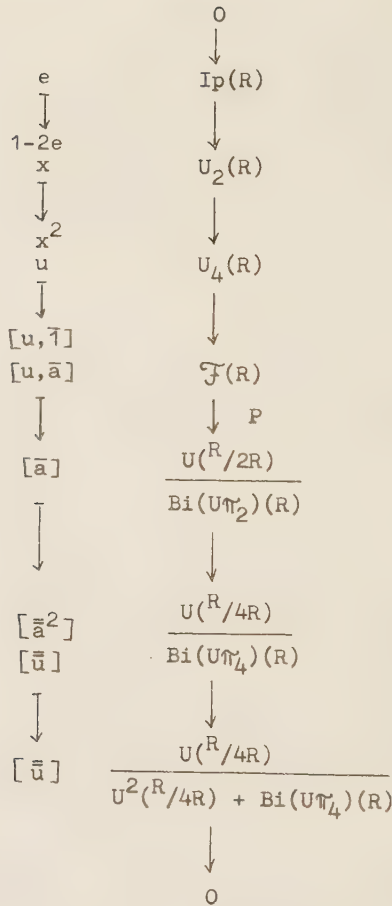
$$\overline{\overline{a^2b}} \in U(R/4R) \quad \text{und} \quad \overline{\overline{a^2}} = \overline{\overline{(a^2b)^2}} \in U^2(R/4R).$$

Eine kleine Diagrammjagd zeigt, daß die Folge (3.33.) auch bei $U(R)/U^2(R)$ exakt ist.

Der letzte Term von (3.33.) ist schließlich so gewählt, daß die Folge mit einem Epimorphismus endet.

C. Small hat in [39] die Frage untersucht, wie sich die Gruppen $\mathcal{N}(R)$ und $\mathcal{F}(R)$ zueinander verhalten. Unter der Voraussetzung, daß 2 ein Nicht-Nullteiler ist, können wir auch dazu allgemeinere Resultate anbieten. Während im ersten Abschnitt dieses Paragraphen der Homomorphismus D gegeben und sein Kern gesucht war, ist nun gewissermaßen der Kern $\mathcal{N}(R)$ gegeben und der zugehörige Homomorphismus gesucht. Die Lösung erhalten wir vollkommen symmetrisch zu (3.33.).

(3.36.) Satz. Ausgehend von der Zeile des Diagrammes (3.29.), in welcher die Picard-Invariante steht, findet man die exakte 7-Term-Folge



Bezeichnung. Der Homomorphismus P kommt folgendermaßen zustande :

Aus der fünften Spalte des Diagrammes (3.29.) ergibt sich ein Isomorphismus

$$\frac{U(R/2R)}{Bi(U\pi_2)(R)} \xrightarrow{\sim} Ke(Ke(\xi^*)) \xrightarrow{sign^*} Pic(R) ,$$

längs dem wir identifizieren. Damit ist klar, daß

pic_R F über $\frac{U(R/2R)}{Bi(U\pi_2)(R)}$ faktorisiert. Diese

Faktorisierung führt zum kommutativen Diagramm

$$\begin{array}{ccc} \mathcal{F}(R) & \xrightarrow{F} & \mathcal{Q}(R) \\ P \downarrow & & \downarrow pic_R \quad (3.37.*) \\ \frac{U(R/2R)}{Bi(U\pi_2)(R)} & \hookrightarrow & Ke(\xi^*) . \end{array}$$

Man kann P also die "Picard-Invariante der freien quadratischen Erweiterungen von R " nennen.

(3.37.) Proposition. Sei P der eben definierte Homomorphismus. Für $[u, \bar{a}] \in \mathcal{F}(R)$ gilt dann $P[u, \bar{a}] = [\bar{a}]$.

Beweis von (3.37.). Für eine treuflache R -Algebra S betrachten wir folgendes kommutative Diagramm

$$\begin{array}{ccccccc} 0 & \longrightarrow & Ip(S) & \xrightarrow{\det} & U(S) & \xrightarrow{\tau} & W(S) \longrightarrow 0 \\ & & \downarrow \alpha' & & \downarrow id & & \downarrow (u^2, \bar{u}) \\ 0 & \longrightarrow & U_2(S) & \xrightarrow[S]{} & U(S) & \xrightarrow[\sigma]{} & Bi(U\pi_2)(S) \longrightarrow 0 \end{array}$$

Dadurch ist ein Morphismus zwischen kurzen exakten Folgen von Prägarben bestimmt. Die obere Folge ist

diejenige aus (3.14.), die untere Folge ist die mittlere Spalte von (3.10.).

Da die Čechschen Kohomologiefunktoren einen "exakten universellen δ -Funktorkomplex" bilden (2.40.), führt dies zu einem Morphismus zwischen den langen Kohomologiefolgen. Mit (3.14.) und (3.29.) heißt dies, daß in folgendem Diagramm die großen Vierecke kommutieren

$$\begin{array}{ccccccc}
 0 & \longrightarrow & I_p(R) & \longrightarrow & U(R) & \longrightarrow & \check{H}^0(R, W) & \longrightarrow & \mathcal{Q}(R) \\
 & & \downarrow \alpha' & & \downarrow \text{id} & & \downarrow \check{H}^0(R, \pi) & \searrow \text{kan} & \downarrow \text{pic}_R \\
 & & & & & & & \mathcal{F}(R) & \\
 & & & & & & & \downarrow P & \\
 & & & & & & & U(R/2R) & \\
 & & & & & & \nearrow \text{kan} & \downarrow & \\
 0 & \longrightarrow & U_2(R) & \longrightarrow & U(R) & \longrightarrow & U(R/2R) & \longrightarrow & \text{Ke}(\xi^*)
 \end{array}$$

Betrachtet man die Beschreibungen von $\check{H}^0(R, W)$ und $\check{H}^0(R, \text{Bi}(U\pi_2))$ in (3.14.) bzw. (3.26.), so ist klar, daß $\check{H}^0(R, \pi)(u, \bar{a}) = \bar{a}$ ist. Deshalb ist $P[u, \bar{a}] = [\bar{a}]$.

(3.38.) Bemerkung. Ist 2 in R ein Nicht-Nullteiler, so ist

$$\begin{array}{ccc}
 R[C_2] & \xrightarrow{\epsilon} & R \\
 \text{sign} \downarrow & & \downarrow \pi_2 \\
 R & \xrightarrow{\pi_2} & R/2R
 \end{array}$$

ein Faserprodukt kommutativer Ringe (vgl. [16]).

Mit Hilfe von Milnors Beschreibung von $\text{Pic}(R[C_2])$ kann man den "verbindenden Homomorphismus"
 $U(R/2R) \longrightarrow \text{Ke}(\xi^*)$, welcher bei der Konstruktion von P vorkam, explizit angeben.

Beweis von (3.36.). Die ersten beiden Pfeile sind wie in (3.29.). Der dritte und der vierte Pfeil machen folgendes Diagramm kommutativ (3.20., 3.37.)

$$\begin{array}{ccccc}
 & & U_4(R) & & \\
 & & \downarrow & \searrow N & \\
 u & & \mathcal{F}(R) & \xrightarrow{\quad} & \mathcal{Q}(R) \\
 \downarrow & & \downarrow P & & \downarrow \text{pic}_R \\
 [u, \tau] & & \frac{U(R/2R)}{\text{Bi}(U\pi_2)(R)} & \xrightarrow{\quad} & \text{Ke}(\xi^*)
 \end{array}$$

Die Folge (3.36.) ist — wie man nun sieht — vollkommen analog zu (3.33.) gebildet. Deshalb ist auch sie exakt.

(3.39.). Aus dem Diagramm (3.37.*) erkennt man, daß $\text{Ke}(P) = \mathcal{N}(R)$ ist. Indem man die Folge (3.36.) an der Stelle $\mathcal{F}(R)$ aufbricht, gewinnt man daher eine exakte Folge

$$0 \longrightarrow \mathcal{N}(R) \longrightarrow \mathcal{F}(R) \xrightarrow{P} \frac{U(R/2R)}{\text{Bi}(U\pi_2)(R)} \longrightarrow \dots$$

Damit haben wir also ein Maß dafür gefunden, wie

stark die Gruppen $\mathcal{N}(R)$ und $\mathcal{F}(R)$ voneinander abweichen.

Bei Small [39] findet man an dieser Stelle nur ein Kriterium für die Gleichheit der beiden Gruppen, welches wir aus unserer Folge leicht ableiten können.

(3.40.) Folgerung. (vgl. [39] Corollary 4)

(2 ist als Nicht-Nullteiler vorausgesetzt !)

Die Untergruppe $\mathcal{N}(R) \hookrightarrow \mathcal{F}(R)$ stimmt genau dann mit $\mathcal{F}(R)$ überein, wenn für alle $a \in R$ gilt:
 $(\exists u \in U(R) : a^2 - u \in 4R) \implies (\exists v \in U(R) : a - v \in 2R).$
 Insbesondere ist $\mathcal{N}(R) = \mathcal{F}(R)$, wenn 2 in R invertierbar ist.

Beweis. $\mathcal{N}(R) = \mathcal{F}(R) \iff P = 0 \iff$

$(\forall a \in R, u \in U(R) : a^2 - u \in 4R \implies \bar{a} \in \text{Bi}(U\pi_2)(R)).$

In (3.34.) und (3.40.) haben wir jeweils die bekannten Resultate als Folgerungen aus unseren Ergebnissen gewonnen. Vergleicht man die beiden, so stellt man fest, daß bisher nur zwei Extremfälle betrachtet wurden.

Beim Diskriminanten-Morphismus D war es der Fall $\text{Ke}(D) = 0$, bei P war es das andere Extrem : $P = 0$. Mit den exakten Folgen (3.33.) und (3.36.) haben wir uns von diesen Spezialfällen gelöst und können nun

ganz allgemein die Kerne und Bilder der Diskriminante bzw. der Picard-Invariante der freien quadratischen Erweiterungen von R beschreiben. Beispielsweise lassen sich damit auch Kriterien dafür angeben, daß die beiden anderen Extremfälle auftreten, was wir zum Abschluß dieses Paragraphen noch tun wollen.

(3.41.) Folgerung. 2 sei ein Nicht-Nullteiler in R .

a.) P ist genau dann injektiv, wenn für alle $u \in U(R)$ gilt:

$$(u - 1 \in 4R) \implies (\exists v \in U(R) : v - 1 \in 2R \text{ und } v^2 = u).$$

b.) Genau dann hat jede freie quadratische Erweiterung eine triviale Diskriminante, wenn für alle $u \in U(R)$ gilt:

$$(\exists a \in R : a^2 - u \in 4R) \implies (\exists v \in R : v^2 = u).$$

Beweis. a.) $P(R)$ injektiv $\iff \mathcal{N}(R) = 0 \iff U_2^2(R) \supseteq U_4(R)$.

b.) $\text{Ke}(\text{dis}_R) = \mathcal{F}(R) \iff D = 0 \iff$

$$(\forall a \in R, u \in U(R) : a^2 - u \in 4R \implies u \in U_2^2(R)).$$

Anhang: Eine exakte Folge von C. Small

Alle Ergebnisse über die Gruppen $\mathcal{F}(R)$ und $\mathcal{M}(R)$ haben wir aus dem Diagramm (3.29.) gewonnen. Damit sind die Möglichkeiten dieses bemerkenswerten Diagrammes aber noch nicht erschöpft.

C. Small [38] hat die exakte Folge

$$0 \longrightarrow \mathcal{F}(R) \longrightarrow \mathcal{Q}(R) \xrightarrow{\det_R} \text{Pic}_{(2)}(R) \longrightarrow \frac{U(R/4R)}{U^2(R/4R) + (U\pi_4)(R)}$$

angegeben und damit das Bild der Determinante, also auch die R -Modulstrukturen quadratischer Erweiterungen von R , beschrieben.

Es zeigt sich, daß auch diese Folge aus (3.29.) abgeleitet werden kann. Während die seltsame Form des letzten Terms bei Smalls ad-hoc-Konstruktion nicht befriedigend erklärbar ist, läßt sich bei der Herleitung aus (3.29.) genau verfolgen, wie sie zustande kommt. Außerdem wird Smalls Folge dabei um 2 Terme verlängert und endet dann mit einem Epimorphismus.

Dies soll in diesem Abschnitt skizziert werden.

Da für die Kokern-Prägarben aus (3.10.) die Bestimmung der ersten Čechschen Kohomologiegruppen Schwierigkeiten macht, gehen wir zum Diagramm der assoziierten Garben über. Wir wenden also auf (3.10.)

den Funktor $\# : \mathcal{P} \longrightarrow \mathcal{S}$ an und erhalten so ein kommutatives Diagramm von Garben mit exakten Zeilen und Spalten (2.40.4.).

Bei $S \in \underline{\mathbf{R-Alg-tf}}$ hat es folgende Gestalt

(3.42.).

$$\begin{array}{ccccccc}
 & 0 & & 0 & & 0 & \\
 & \downarrow & & \downarrow & & \downarrow & \\
 0 & \longrightarrow & \mathrm{Ip}(S) & \longrightarrow & \mathrm{U}_2(S) & \longrightarrow & \mathrm{U}_4(S) \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & \mu_2(S) & \longrightarrow & \mathrm{U}(S) & \longrightarrow & \mathrm{U}(S) \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & \mathrm{Bi}(\mu_2^4)(S) & \longrightarrow & \mathrm{U}(S/2S) & \longrightarrow & \mathrm{U}(S/4S) \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 0 & & 0 & & 0
 \end{array}$$

$$\begin{array}{ccccc}
 e & \longmapsto & 1-2e & u & \longmapsto & u^2 & v \\
 \downarrow & & & \downarrow & & & \downarrow \\
 1-2e & & & u & \longmapsto & u^2 & v \\
 \downarrow & & & \downarrow & & & \downarrow \\
 \bar{u} & \longmapsto & \bar{u} & \longmapsto & \bar{u}^2 & \bar{v} & .
 \end{array}$$

Die einzelnen Teile dieser Aussage haben wir in (2.42.), (3.20.), (3.23.), (3.25.) und (3.26.) bewiesen.

(3.43.) Definition der Garben-Kohomologie.

Die Garben-Kohomologie über $\mathcal{O}_R$ wird von den abgeleiteten Funktoren des linksexakten Auswertungsfunktors

$$\mathcal{S} \ni F \longmapsto F(R) \in \underline{\text{Ab}}$$

gebildet. Diese bezeichnen wir mit $H^n(R, -)$, $n \geq 0$.

Für die ersten beiden gilt (vgl. [2] II.3.) :

$$H^0(R, -) = \check{H}^0(R, -) \circ \iota = \text{"Auswertung bei } R \text{"}$$

$$H^1(R, -) \simeq \check{H}^1(R, -) \circ \iota .$$

Anstelle von (3.29.) betrachten wir nun das entsprechende Diagramm der Garben-Kohomologie von (3.42.) , identifizieren dabei aber längs des Isomorphismus $H^1(R, -) \simeq \check{H}^1(R, -) \circ \iota$. Auf diese Weise wird (3.29.) zu folgendem kommutativen Diagramm mit exakten Zeilen und Spalten ergänzt :

(3.44.).

$$\begin{array}{ccccccc}
 & & & 0 & & 0 & & 0 \\
 & & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & \text{Ip}(R) & \longrightarrow & \text{U}_2(R) & \longrightarrow & \text{U}_4(R) \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & \mu_2(R) & \longrightarrow & \text{U}(R) & \longrightarrow & \text{U}(R) \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & & 0 & \longrightarrow & \text{Bi}\mu_2\pi_2^4(R) & \longrightarrow & \text{U}^R(2R) & \longrightarrow & \text{U}^R(4R) \\
 & & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & \text{Ip}(R) & \longrightarrow & \text{U}_2(R) & \longrightarrow & \text{U}_4(R) & \longrightarrow & \mathcal{Q}(R) & \xrightarrow{\text{pic}_R} & \mathcal{A}_2(R) & \xrightarrow{(\)^2} & \mathcal{A}_4(R) \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & \text{dis}_R & \downarrow & & \downarrow \\
 0 & \longrightarrow & \mu_2(R) & \longrightarrow & \text{U}(R) & \longrightarrow & \text{U}(R) & \longrightarrow & \text{Dis}(R) & \longrightarrow & \text{Pic}(R) & \xrightarrow{(\)^2} & \text{Pic}(R) \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & \text{Bi}\mu_2\pi_2^4(R) & \longrightarrow & \text{U}^R(2R) & \longrightarrow & \text{U}^R(4R) & \longrightarrow & \check{H}^1(\text{Bi}\mu_2\pi_2^4) & \longrightarrow & \text{Pic}^R(2R) & \longrightarrow & \text{Pic}^R(4R) .
 \end{array}$$

An dieser Stelle soll zunächst einmal die Bedeutung der Symbole $\mathcal{A}_2(R)$ und $\mathcal{A}_4(R)$ geklärt werden.

(3.45.) Definition. Für einen kommutativen Ring R sei $\mathcal{A}_2(R)$ folgende Kategorie :

Ihre Objekte sind Paare (P, π) aus einem invertierbaren R -Modul P und einem R -Isomorphismus $\pi : P/2P \xrightarrow{\sim} R/2R$. Morphismen $f : (P, \pi) \rightarrow (P', \pi')$ sind R -Homomorphismen $f : P \rightarrow P'$, für welche das Dreieck

$$\begin{array}{ccc} P/2P & \xrightarrow{\bar{f}} & P'/2P' \\ \pi \searrow & & \swarrow \pi' \\ & R/2R & \end{array} \quad \text{kommutiert.}$$

$\mathcal{A}_2(R)$ sei die Menge der Isomorphieklassen von $\mathcal{A}_2(R)$.

Man prüft schnell nach, daß die Vorschrift

$$[P, \pi] [P', \pi'] := [P \otimes_R P', \pi \otimes_{R/2R} \pi']$$

auf ihr die Struktur einer abelschen Gruppe definiert.

$[R, \text{id}]$ ist das neutrale Element, und das zu

$[P, \pi]$ inverse Element ist

$$[R\text{-Mod}(P, R), R\text{-Mod}(P, R) \otimes_{R/2R} R/2R \ni f \otimes \bar{1} \mapsto \bar{f} \pi^{-1}(\bar{1}) \in R/2R]$$

$\mathcal{A}_4(R)$ ist auf analoge Weise gebildet.

Damit ist es nun intuitiv klar, wie diejenigen Pfeile von (3.44.) operieren, die wir aus (3.29.) noch nicht kennen.

Aber es ist auch klar, daß es noch einige Mühe kostet, wenn man nachweisen will, daß diese Homomorphismen tatsächlich durch $\check{H}^1(R, -)$ aus (3.42.) hervorgehen.

Die Isomorphie $\check{H}^1(R, U(\sim/2-)) \simeq \text{Pic}(R/2R)$ beruht im wesentlichen darauf, daß zu jeder "Zariski-Überdeckung" T von $R/2R$ eine "Zariski-Überdeckung" S von R existiert mit $S/2S \simeq T$ (vgl. [13] Theorem 5.6.) : Ist $T = \bigcap_{i=1}^n (R/2R)_{a_i}$ mit $a_1, \dots$,

$a_n \in R$, so kann man $S = R_2 \times R_{a_1} \times \dots \times R_{a_n}$ wählen.

Für $\check{H}^1(R, U_2)$ haben wir bereits die Beschreibung $\check{H}^1(R, U_2) \simeq \text{Ke}(\varepsilon^*)$ angegeben (vgl. 3.8.). Die dabei benutzte zulässige Struktur $\underline{T}$ orientierte sich an der zu U_2 isomorphen Garbe $\text{Ke}(U\varepsilon)$. Die Isomorphie $\check{H}^1(R, U_2) \simeq \mathcal{A}_2(R)$ erhält man dagegen mit Hilfe einer zulässigen Struktur $\underline{A}_2$, die man findet, wenn man von U_2 selbst ausgeht: Der zugehörige Graph besteht aus einem Pfeil $\pi : 1 \rightarrow 0$, die Funktoren sind

$$F_1^S : \underline{S\text{-Mod}} \rightarrow \underline{S\text{-Mod}}, \quad M \mapsto M/2M, \quad f \mapsto \bar{f}$$

$$F_0^S : \underline{S\text{-Mod}} \rightarrow \underline{S\text{-Mod}}, \quad M \mapsto S/2S, \quad f \mapsto \text{id.}$$

Damit sind dann verzerrte Formen des Objektes

$(R, id) \in \underline{A}_2(R)$ zu betrachten.

aus (3.44.) die Folge von Small zu gewinnen,

sehen wir von folgendem Viereck aus

$$\begin{array}{ccc} \mathcal{A}_2(R) & \xrightarrow{(\quad)^2} & \mathcal{A}_4(R) \\ \downarrow & & \downarrow \\ \text{Pic}(R) & \xrightarrow{(\quad)^2} & \text{Pic}(R) \end{array} .$$

Die senkrechten Pfeile ergänzen wir zu kurzen exakten

Folgen, indem wir die Kerne davorschalten und die

Pfeile einschränken. Zusammen mit den Kernen und Ko-

kernen der waagrechten Pfeile bilden sie folgendes

Commutative Diagramm mit exakten Zeilen und Spalten

(3.46.)

$$\begin{array}{ccccccc} & 0 & & 0 & & 0 & \\ & \downarrow & & \downarrow & & \downarrow & \\ \rightarrow & \frac{\mathcal{F}(R)}{\mathcal{N}(R)} & \rightarrow & \frac{U(R/2R)}{\text{Bi}(U\pi_2)(R)} & \rightarrow & \frac{U(R/4R)}{\text{Bi}(U\pi_4)(R)} & \rightarrow \frac{U(R/4R)}{U^2(R/4R) + \text{Bi}U\pi_4(R)} \rightarrow 0 \\ & \downarrow & & \downarrow & & \downarrow & \\ \rightarrow & \frac{\mathcal{L}(R)}{\mathcal{N}(R)} & \rightarrow & \mathcal{A}_2(R) & \xrightarrow{(\quad)^2} & \mathcal{A}_4(R) & \rightarrow \frac{\mathcal{A}_4(R)}{\mathcal{A}_2^2(R)} \rightarrow 0 \\ & \downarrow & & \downarrow & & \downarrow & \\ \rightarrow & \text{Pic}_{(2)}(R) & \rightarrow & \text{Pic}_2(R) & \xrightarrow{(\quad)^2} & \text{Pic}_4(R) & \rightarrow \frac{\text{Pic}_4(R)}{\text{Pic}_2^2(R)} \rightarrow 0 \\ & \downarrow & & \downarrow & & \downarrow & \\ & 0 & & 0 & & 0 & \end{array}$$

$$\begin{aligned}
 \text{Dabei bezeichnen} \quad \text{Pic}_2(R) &: = \text{Ke}(\text{Pic}(\pi_2)) \\
 \text{Pic}_4(R) &: = \text{Ke}(\text{Pic}(\pi_4)) \\
 \text{Pic}_{(2)}(R) &: = \text{Pic}_2(R) \cap \text{Ke}(\text{Pic}(\pi_2)^2).
 \end{aligned}$$

Die Exaktheit der oberen Zeile zeigt (3.36.), diejenige der mittleren Zeile erkennt man aus (3.44.), und die Exaktheit der unteren Zeile ist klar. Also sind die Kerne und Kokerne der Zeilen richtig beschrieben. Aus der Konstruktion des Diagrammes ergibt sich nun unmittelbar die Kommutativität und die Exaktheit der Spalten.

(3.47.) Smalls exakte Folge.

Das "Schlangen-Lemma" ([6]Chap.1., Prop.4.7.) gibt uns im Diagramm (3.46.) einen verbindenden Homomorphismus. (Er ist gestrichelt eingetragen.) So erhalten wir die exakte Folge

$$\begin{aligned}
 0 \longrightarrow \mathcal{F}(R) \longrightarrow \mathcal{Q}(R) \xrightarrow{\det_R} \text{Pic}_{(2)}(R) \longrightarrow \frac{U(R/4R)}{U^2(R/4R) + \text{Bi}U\pi_4(R)} \\
 \longrightarrow \frac{\mathcal{A}_4(R)}{\mathcal{A}_2^2(R)} \longrightarrow \frac{\text{Pic}_4(R)}{\text{Pic}_2^2(R)} \longrightarrow 0.
 \end{aligned}$$

Die übliche Diagrammjagd des Schlangen-Lemmas
läßt sich in (3.46.) folgendermaßen skizzieren:

Sei $[P] \in \text{Pic}_{(2)}(R)$ mit Isomorphismen

$$\mu: P \otimes P \xrightarrow{\sim} R, \quad \pi: P \otimes^R R/2R \xrightarrow{\sim} R/2R, \text{ und es sei}$$

$$x \in P \text{ mit } \pi(\bar{x}) = \bar{1}.$$

$$\begin{array}{c} \frac{U(R/4R)}{U^2(R/4R) + \text{Bi}(U\pi_4)(R)} \\ \downarrow \\ [\overline{\mu(x \otimes x)}] \longmapsto [\overline{\mu(x \otimes x)}] \\ \downarrow \\ [P, \pi] \longmapsto [P \otimes P, P \otimes P \otimes^R R/4R \xrightarrow{\sim} R/4R] \\ \quad \quad \quad x \otimes x \otimes \bar{1} \longleftarrow \bar{1} \\ \downarrow \quad \quad \downarrow \\ [P] \longmapsto [P] \longmapsto [R] \\ \cap \end{array}$$

$$\text{Pic}_{(2)}(R)$$

Dies zeigt, daß der verbindende Homomorphismus tat-
sächlich mit dem von C.Small definierten Homomorphis-
mus übereinstimmt.

Kapitel 4

FREIE QUADRATISCHE ERWEITERUNGEN VON ORDNUNGEN IN QUADRATISCHEN ZAHLKÖRPERN

Mit Hilfe der Ergebnisse von Kapitel 3 bestimmen wir nun die $GF(2)$ -Dimensionen der Gruppen $\mathcal{F}$ und $\mathcal{N}$ für Ordnungen in quadratischen Zahlkörpern.

§ 0 Grundlagen und Bezeichnungen

In diesem Abschnitt schildern wir, um welche Ringe es sich bei Ordnungen in quadratischen Zahlkörpern handelt, wie sich ihre Elemente darstellen lassen und was über ihre Einheitengruppen bekannt ist. Im übrigen verweisen wir auf das Lehrbuch von Borevič und Šafarevič ([8] Kap. 2. § 7), in dem all diese Ergebnisse bewiesen sind und die Begriffe in geeigneter Allgemeinheit definiert werden.

(4.1.). Quadratische Zahlkörper sind Erweiterungen des Körpers $\mathbb{Q}$ der rationalen Zahlen vom Grad 2. Sie lassen sich bijektiv quadratfreien ganzrationalen Zahlen $d \neq 1$ zuordnen. Dabei heißt $d \in \mathbb{Z}$ quadratfrei, wenn d von keinem Quadrat einer Primzahl ge-

teilt wird, und einem quadratfreien $d \neq 1$ entspricht der Körper $\mathbb{Q}(\sqrt{d})$.

Dies kann man auch aus unseren Ergebnissen über freie quadratische Erweiterungen ableiten. Mit Hilfe von (3.35.) erhält man die Bijektion

$$\{d \in \mathbb{Z} \mid d \text{ quadratfrei}\} \xrightarrow{\sim} U(\mathbb{Q})/U^2(\mathbb{Q}) \xrightarrow{\sim} \mathcal{F}(\mathbb{Q}) \xrightarrow{\sim} \mathcal{Q}(\mathbb{Q}) .$$

$$d \longmapsto [d] \longmapsto [d, \bar{0}] \longmapsto F[d, \bar{0}]$$

Für $d \neq 1$ ergibt sich $F[d, \bar{0}] = F[4d, \bar{0}] = [\mathbb{Q}[x]/(x^2-d)]$,
 $d = 1$ entspricht $F[1, \bar{0}] = F[1, \bar{1}] = [\mathbb{Q}[x]/(x^2-x)]$. Da die triviale quadratische Erweiterung jedoch kein Körper ist, ist $d = 1$ auszuschließen.

(4.2.). Eine Ordnung im quadratischen Zahlkörper $\mathbb{Q}(\sqrt{d})$ ist ein Unterring, dessen additive Gruppe frei vom Rang 2 ist. Der Ring der ganzen algebraischen Zahlen in $\mathbb{Q}(\sqrt{d})$ ist eine Ordnung. Sie enthält alle anderen Ordnungen von $\mathbb{Q}(\sqrt{d})$ und wird deshalb Maximalordnung oder auch Hauptordnung von $\mathbb{Q}(\sqrt{d})$ genannt.

Wir wählen dafür die Bezeichnung A^d .

Bei der Beschreibung einer Basis von A^d über $\mathbb{Z}$ sind zwei Fälle zu unterscheiden:

$\{1, \omega\}$ ist eine $\mathbb{Z}$ -Basis von A^d , wobei

$$\omega = \begin{cases} \sqrt{d} & , \text{ falls } d \equiv 2,3(4) \\ \frac{1 + \sqrt{d}}{2} & , \text{ falls } d \equiv 1(4) \end{cases} .$$

Damit lassen sich nun die Ordnungen von $\mathbb{Q}(\sqrt{d})$ bijektiv natürlichen Zahlen $q \geq 1$ zuordnen.

Der Zahl q entspricht die Ordnung mit der $\mathbb{Z}$ -Basis $\{1, q\omega\}$. Wir bezeichnen sie A_q^d . q gewinnt man aus ihr als Index von A_q^d in $A^d = A_1^d$ zurück.

Speziell ist also für $t \in \mathbb{Z} \setminus \mathbb{Z}^2$ der Ring $\mathbb{Z}[\sqrt{t}]$ eine Ordnung. Und zwar gibt es eine eindeutige Darstellung der Form $t = dr^2$ mit einer quadratfreien ganzrationalen Zahl $d \neq 1$ und einer natürlichen Zahl $r \geq 1$. Damit

$$\text{ist dann } \mathbb{Z}[\sqrt{t}] = \begin{cases} A_r^d, & \text{falls } d \equiv 2,3(4) \\ A_{2r}^d, & \text{falls } d \equiv 1(4) \end{cases}.$$

(4.3.). Ein Element $a \in A_q^d$ ist genau dann eine Einheit in A_q^d , wenn seine Norm ± 1 ist. Über die Struktur der Einheitengruppe besagt der Dirichletsche Einheitensatz ([8] Kap. 2 § 4)

$$U(A_q^d) \simeq W \times \mathbb{Z}^r \quad \text{mit } r = \begin{cases} 0 & \text{für } d < 0 \\ 1 & \text{für } d > 0 \end{cases}.$$

Dabei entspricht W der Gruppe der Einheitswurzeln in A_q^d .

Im reell-quadratischen Fall ($d > 0$) gibt es in A_q^d genau eine Einheit ε_q^d mit den Eigenschaften

$$\varepsilon_q^d > 1 \quad \text{und} \quad U(A_q^d) = \{ \pm (\varepsilon_q^d)^n \mid n \in \mathbb{Z} \}.$$

ε_q^d heißt Grundeinheit von A_q^d , ihre Basisdarstellung

bezeichnen wir mit

$$\varepsilon_q^d = (\varepsilon_q^d)_1 + (\varepsilon_q^d)_2 \cdot q\omega, \quad (\varepsilon_q^d)_i \in \mathbb{Z}.$$

Für die Hauptordnungen der imaginärquadratischen Zahlkörper ($d < 0$) haben die Einheitengruppen folgende Gestalt

$$U(A_1^d) = \begin{cases} \{\pm 1, \pm \sqrt{-1}\} & \text{für } d = -1 \\ \{\pm 1, \frac{1}{2}(\pm 1 \pm \sqrt{-3})\} & \text{für } d = -3 \\ \{\pm 1\} & \text{sonst} \end{cases}.$$

§ 1 Die Gruppe der freien quadratischen Erweiterungen von A_q^d

(4.4.). Von nun an halten wir eine quadratfreie ganzrationale Zahl $d \neq 1$ und eine natürliche Zahl $q \geq 1$ fest. Für die Ordnung A_q^d wollen wir die Struktur der Gruppe $\mathcal{F}(A_q^d)$ bestimmen. Dazu haben wir — da A_q^d ein Integritätsring der Charakteristik 0 ist — die exakte Folge (vgl. 3.33., 3.34.)

$$0 \rightarrow \text{Bi}(\mu_2^4)(A_q^d) \rightarrow \mathcal{F}(A_q^d) \xrightarrow{D(A_q^d)} U/U^2(A_q^d) \rightarrow U/U^2(A_q^d/4A_q^d).$$

Da alle Gruppen der Folge den Exponent 2 haben, heißt "Strukturbestimmung" nichts anderes als Bestimmung der $\text{GF}(2)$ -Dimensionen.

(4.5.) Proposition.

$$\text{GF}(2) - \dim \text{Ke } D(A_q^d) = \begin{cases} 1, & \text{falls } d \equiv 1(4) \text{ und } q \equiv 2(4) \\ 0 & \text{sonst} \end{cases}$$

Beweis. Wir führen den Beweis in mehreren Schritten und wenden jeweils (3.34.) an.

a.) Sei zunächst $d \equiv 2,3(4)$, und für $a \in A_q^d$ gelte $a^2 - 1 \in 4A_q^d$. $a = a_1 + a_2q\sqrt{d}$ sei die Basisdarstellung von a mit Koeffizienten in $\mathbb{Z}$.

Wegen der Eindeutigkeit der Basisdarstellung erhält man folgende Kongruenzen ganzrationaler Zahlen

$$(i) \quad a_1^2 + a_2^2 q^2 d - 1 \equiv 0(4)$$

$$(ii) \quad 2 a_1 a_2 \equiv 0(4) .$$

Aus (ii) folgt: $a_1 \equiv 0(2)$ oder $a_2 \equiv 0(2)$. Nehmen wir an $a_1 \equiv 0(2)$, so erhalten wir durch Einsetzen in (i) $(a_2 q)^2 d \equiv 1(4)$, und daraus schließt man $d \equiv 1(4)$. Dies steht im Widerspruch zu unserer Voraussetzung a.). Also ist $a_1 \equiv 1(2)$, $a_2 \equiv 0(2)$, d.h. $a - 1 \in 2 A_q^d$.

b.) Sei nun $d \equiv 1(4)$, und $\tilde{d} \in \mathbb{Z}$ sei so gewählt, daß $d = 1 + 4\tilde{d}$ ist. $a = a_1 + a_2q\omega$ sei ein Element von A_q^d .

Eine Zwischenüberlegung zeigt:

$$\omega^2 = \frac{1}{4}(1 + 2\sqrt{d} + d) = \tilde{d} + \omega ;$$

$$a^2 - 1 = (a_1^2 + a_2^2 q^2 \tilde{d} - 1) + (2a_1 a_2 + a_2^2 q) q \omega ;$$

$$a^2 - 1 \in 4A_q^d \iff (i) \quad a_1^2 + a_2^2 q^2 \tilde{d} - 1 \equiv 0(4)$$

$$(ii) \quad 2 a_1 a_2 + a_2^2 q \equiv 0(4) .$$

Wir wollen nun zeigen

$$(\alpha) \quad q \equiv 1(2) \implies (a^2-1 \in 4A_q^d \implies a-1 \in 2A_q^d)$$

$$(\beta) \quad q \equiv 0(4) \implies (a^2-1 \in 4A_q^d \implies a-1 \in 2A_q^d) \quad .$$

(α) Sei $q \equiv 1(2)$ und $a^2-1 \in 4A_q^d$. Betrachtet man (ii) modulo 2, so sieht man $a_2^2 \equiv 0(2)$, also $a_2 \equiv 0(2)$. Die Kongruenz (i) zeigt deshalb $a_1^2 \equiv 1(4)$, also $a_1 \equiv 1(2)$. Wie oben ist daher $a-1 \in 2A_q^d$.

$$(\beta) \quad \text{Sei } q \equiv 0(4) \quad \text{und } a^2-1 \in 4A_q^d .$$

(ii) $\implies 2 a_1 a_2 \equiv 0(4) \implies (a_1 \equiv 0(2) \text{ oder } a_2 \equiv 0(2))$. $a_1 \equiv 0(2)$ ist aber nicht möglich, da sonst (i) die Kongruenz $-1 \equiv 0(4)$ ergäbe. Somit gilt $a_1 \equiv 1(2)$ und $a_2 \equiv 0(2)$.

(γ) Sei nun $q \equiv 2(4)$. Dann gilt

$$\begin{aligned} a^2-1 \in 4A_q^d &\iff (i) \quad a_1^2 + a_2^2 q^2 \tilde{d} -1 \equiv 0(4) \\ &\quad (ii) \quad 2 a_1 a_2 + a_2^2 q \equiv 0(4) \\ &\iff (i) \quad a_1^2 \equiv 1(4) \\ &\quad (ii) \quad 2 (a_1 a_2 + a_2^2) \equiv 0(4) \\ &\iff (i) \quad a_1 \equiv 1(2) \\ &\quad (ii) \quad a_2 + a_2^2 \equiv 0(2) \\ &\iff a_1 \equiv 1(2) \end{aligned}$$

$Bi(\mu_2 \pi_2^4)(A_q^d)$ enthält deshalb genau die beiden Elemente $\overline{1}$ und $\overline{1 + q\omega}$.

(4.6.) Folgerungen. Als Spezialfälle von (4.5.)

notieren wir:

- a.) Für alle Hauptordnungen A^d ist $D(A^d)$ injektiv.
- b.) Ist $d \equiv 1(4)$, so ist $\text{Ke } D(\mathbb{Z}[\sqrt{d}]) \neq 0$.
- c.) Für $t \in \mathbb{Z} \setminus \mathbb{Z}^2$ ist $\text{Ke } D(\mathbb{Z}[\sqrt{t}])$ genau dann $\neq 0$, wenn $t \equiv 1(4)$ ist.

Beweis. a.) Klar. b.) $\mathbb{Z}[\sqrt{d}] = A_2^d$.

c.) " $\implies$ " : Sei $D(\mathbb{Z}[\sqrt{t}])$ nicht injektiv.

Außerdem sei $t = dr^2$ eine Zerlegung von t gemäß (4.2.). (4.5.) zeigt, daß $d \equiv 1(4)$ gelten muß.

Daher ist $\mathbb{Z}[\sqrt{t}] = A_{2r}^d$ (vgl. 4.2.). Da $D(A_{2r}^d)$

nicht injektiv ist, folgt $2r \equiv 2(4) \implies r \equiv 1(2)$

$\implies r^2 \equiv 1(4) \implies t \equiv 1(4)$. " $\Leftarrow$ " : Sei nun $t \equiv 1(4)$ und $t = dr^2$ gemäß (4.2.) zerlegt.

$dr^2 \equiv 1(4) \implies r^2 \equiv 1(4)$

$\implies d \equiv 1(4)$ und ($r \equiv 1(4)$ oder $r \equiv 3(4)$)

$\implies d \equiv 1(4)$ und $2r \equiv 2(4)$.

$D(\mathbb{Z}[\sqrt{t}]) = D(A_{2r}^d)$ ist daher nicht injektiv.

Nun ist also noch das Bild von $D(A_q^d)$ zu bestimmen.

Dazu betrachten wir zunächst die Quadratklassengruppe $U/U^2(A_q^d)$.

(4.7.) Proposition. a.) Ist $d < 0$, so ist
für alle $q \in \mathbb{N}$ $U/U^2(A_q^d) \simeq \mathbb{Z}/2\mathbb{Z}$.

Die von der Einsklasse $[1]$ verschiedene Klasse
ist $[i]$ für $d = -1$ und $q = 1$. In allen
anderen Fällen ist sie $[-1]$.

b.) Ist $d > 0$, so ist

für alle $q \in \mathbb{N}$ $U/U^2(A_q^d) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Die vier verschiedenen Klassen sind $[\pm 1], [\pm \varepsilon_q^d]$.

(ε_q^d ist dabei die Grundeinheit von A_q^d .)

Beweis. a.) Sei zunächst $d < 0$, $-1 \neq d \neq -3$.

Dann gilt für alle $q \in \mathbb{N}$: $U(A_q^d) = \{\pm 1\}$,

$U^2(A_q^d) = \{+1\}$, $U/U^2(A_q^d) = \{[\pm 1]\}$.

Nun betrachten wir $d = -1$. Für die Hauptordnung

gilt: $U(A^{-1}) = \{\pm 1, \pm i\}$, $U^2(A^{-1}) = \{\pm 1\}$, $U/U^2(A^{-1}) = \{[1], [i]\}$. Für $q \neq 1$ sieht man: $U(A_q^{-1}) = \{\pm 1\}$,

$U^2(A_q^{-1}) = \{1\}$, $U/U^2(A_q^{-1}) = \{[\pm 1]\}$.

Sei schließlich $d = -3$. Die Einheitengruppe der

Hauptordnung ist $U(A^{-3}) = \{\pm 1, \pm \omega, \pm (1-\omega)\}$. Außerdem enthält A_q^d genau dann eines der Elemente $\pm \omega$, $\pm (1-\omega)$, wenn $q = 1$ ist.

$U(A^{-3})$ ist zyklisch, und wie man schnell nachprüft
gilt die Verknüpfungstabelle

n	1	2	3	4	5	6
ω^n	ω	$-1 + \omega$	-1	$-\omega$	$1 - \omega$	1

Daraus erkennt man : $U^2(A^{-3}) = \{-1 + \omega, -\omega, 1\}$,

$$U/U^2(A^{-3}) = \{[\pm 1]\}.$$

Für die anderen Ordnungen in $\mathbb{Q}(\sqrt{-3})$ ist $U(A_q^{-3}) = \{\pm 1\}$,

$$U^2(A_q^{-3}) = \{1\}, \quad U/U^2(A_q^{-3}) = \{[\pm 1]\}.$$

b.) Sei nun $d > 0$. Wie wir wissen, gilt für Ordnungen in reell-quadratischen Zahlkörpern

$$U(A_q^d) = \{\pm (\varepsilon_q^d)^n \mid n \in \mathbb{Z}\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}.$$

$$\text{Deshalb ist } U^2(A_q^d) = \{(\varepsilon_q^d)^{2n} \mid n \in \mathbb{Z}\} \quad \text{und}$$

$$U/U^2(A_q^d) = \{[\pm 1], [\pm \varepsilon_q^d]\}.$$

Im folgenden werden wir uns mit der Frage beschäftigen müssen, welche Elemente von $U/U^2(A_q^d)$ im Bild von D liegen.

(4.8.) Kriterium. R sei ein kommutativer Ring, und 2 sei ein Nicht-Nullteiler in R .

Ist $K \in U/U^2(R)$ und $u \in U(R)$ ein beliebiger Repräsentant von K , so gilt

$$K \in \text{Bi } D(R) \iff \exists a \in R : a^2 - u \in 4R.$$

Beweis. " $\Leftarrow$ " Sei $a \in R$ mit $a^2 - u \in 4R \implies$

$$[u, \bar{a}] \in \mathcal{F}(R) \quad \text{und} \quad K = [u] = D[u, \bar{a}] \in \text{Bi } D(R)$$

(vgl. 3.30.). " $\implies$ " $K \in \text{Bi } D(R)$

$\implies \exists [x, \bar{y}] \in \mathcal{F}(R) : [u] = D[x, \bar{y}] = [x]$

$\implies \exists y \in R ; x, v \in U(R) : y^2 - x \in 4R \text{ und } u = v^2 x$

$\implies [x, \bar{y}] = [v^2 x, \bar{v} y] = [u, \bar{v} y] \in \mathcal{F}(R)$

$\implies \text{für } a := v y \text{ ist } a^2 - u \in 4R.$

Bemerkung. Es ist klar, daß Homomorphismen zwischen Restklassengruppen im allgemeinen nicht diese Eigenschaft haben. Im Beispiel $f : \mathbb{Z} \ni x \mapsto \overline{2x} \in \mathbb{Z}/3\mathbb{Z}$ ist zwar $\overline{1} \in \text{Bi}(f)$, aber der Repräsentant 1 ist nicht von der Form $2x$ mit $x \in \mathbb{Z}$.

In (4.7.) haben wir die Gruppen $U/U^2(A_q^d)$ angegeben.

Als Repräsentanten treten dabei $\pm 1, i, \pm \xi_q^d$ auf.

Für diese Einheiten $u \in U(A_q^d)$ wollen wir nun die

Frage untersuchen:

Gibt es ein $a \in A_q^d$, so daß $a^2 - u \in 4A_q^d$ ist?

Indem man $a^2 - u$ bezüglich der $\mathbb{Z}$ -Basis $\{1, q\omega\}$ darstellt, wird daraus eine Frage nach der Lösbarkeit von Kongruenzen in $\mathbb{Z}$.

(4.9.) Proposition. $u = u_1 + u_2 q\omega$, $u_i \in \mathbb{Z}$ sei eine Einheit der Ordnung A_q^d . Die Klasse $[u] \in U/U^2(A_q^d)$ ist genau dann in $\text{Bi } D(A_q^d)$, wenn das Quadrupel (d, q, u_1, u_2) einem der folgenden Systeme von Kongruenzen genügt :

d	q	u_1	u_2
2(4)	beliebig	1(4)	0(4)
	0(2)	1(4)	2(4)
	1(2)	3(4)	2(4)
3(4)	beliebig	1(4)	0(4)
	0(2)	1(4)	2(4)
	1(2)	3(4)	0(4)
1(4)	beliebig	1(4)	0(4)
	0(4)	1(4)	2(4)
5(16)	1(4)	1(4)	1(4)
		2(4)	3(4)
	3(4)	1(4)	3(4)
		2(4)	1(4)
13(16)	1(4)	0(4)	3(4)
		3(4)	1(4)
	3(4)	0(4)	1(4)
		3(4)	3(4)

(4.10.) Folgerung. Aus der Tabelle (4.9.) erkennt man: Die Klasse $[-1]$ ist genau dann im Bild von $D(A_q^d)$, wenn $d \equiv 3(4)$ und $q \equiv 1(2)$ sind.

Bemerkung. Für die Hauptordnungen A^d , $d > 0$ hat dies bereits Théron gezeigt (vgl. [41] Lemma 3).

Beweis von (4.9.). Es ist eine ganze Reihe von Fallunterscheidungen zu machen.

(4.9.1.) Sei $d \equiv 2(4)$. Nach (4.8.) ist $[u] \in \text{BiD}(A_q^d)$

$$\iff \exists a \in A_q^d : a^2 - u \in 4A_q^d$$

$$\iff \exists a_1, a_2 \in \mathbb{Z} : \left\{ \begin{array}{l} \text{(i)} \quad a_1^2 + a_2^2 q^2 d - u_1 \equiv 0(4) \\ \text{(ii)} \quad 2a_1 a_2 - u_2 \equiv 0(4) \end{array} \right\} \quad (*)$$

$u_2 \equiv 1(2)$: (ii) $\implies 1 \equiv 0(2)$. (*) ist also nicht lösbar.

$u_2 \equiv 0(4)$, $u_1 \equiv 3(4)$, $q \equiv 0(2)$: (i) $\implies a_1^2 \equiv 3(4)$; (*) ist nicht lösbar.

$u_2 \equiv 0(4)$, $u_1 \equiv 3(4)$, $q \equiv 1(2)$: (ii) $\implies a_1 \equiv 0(2)$ oder $a_2 \equiv 0(2)$. Falls $a_1 \equiv 0(2)$ ist, so wird (i) zu $2a_2^2 \equiv 3(4)$; ist $a_2 \equiv 0(2)$, so ergibt (i) $a_1^2 \equiv 3(4)$. In keinem Fall ist also (*) lösbar.

$u_2 \equiv 0(4)$, $u_1 \equiv 1(4)$: $a_1 = 1$, $a_2 = 0$ lösen (*).
 $u_2 \equiv 2(4)$, $u_1 \equiv 1(4)$, $q \equiv 1(2)$: (ii) $\implies a_1 \equiv a_2 \equiv 1(2)$. In (i) eingesetzt ergibt dies $u_1 \equiv 3(4)$, im Widerspruch zur Voraussetzung.

$u_2 \equiv 2(4)$, $u_1 \equiv 1(4)$, $q \equiv 0(2)$: $a_1 = a_2 = 1$ lösen (*).

$u_2 \equiv 2(4)$, $u_1 \equiv 3(4)$, $q \equiv 1(2)$: $a_1 = a_2 = 1$ lösen (*).

$$\underline{u_2 \equiv 2(4)}, \underline{u_1 \equiv 3(4)}, \underline{q \equiv 0(2)} : (i) \implies \\ a_1^2 \equiv 3(4). (*) \text{ ist also nicht lösbar.}$$

Diese Fallunterscheidungen sind vollständig, denn ist u_2 gerade, so kann u_1 nicht auch noch gerade sein. Sonst wäre $\frac{1}{2} \in A_q^d$.

(4.9.2.) Sei $d \equiv 3(4)$. Wir benutzen dasselbe Kriterium (*) wie bei (4.9.1.). Wie dort kann auch der Fall $u_1 \equiv u_2 \equiv 0(2)$ nicht auftreten. Darüber hinaus überlegen wir nun, daß auch $u_2 \equiv 2(4)$, $q \equiv 1(2)$ nicht auftreten kann: Die Norm einer Einheit ist ± 1 , d.h. $u_1^2 - u_2^2 q^2 d = \pm 1$. Seien nun $u_2 \equiv 2(4)$, $q \equiv 1(2)$. In die Gleichung eingesetzt ergibt dies $\pm 1 \equiv u_1^2(4)$. Es ist also nur $+1 = u_1^2 - u_2^2 q^2 d$ möglich. Außerdem ist $u_1 \equiv 1(2)$. Betrachtet man nun diese letzte Gleichung modulo 8, so zeigt sich der Widerspruch $1 \equiv 1 - 4 \cdot 1 \cdot 3 (8)$.

$u_2 \equiv 1(2) : (ii) \implies 1 \equiv 0(2)$. (*) ist nicht lösbar.

$u_2 \equiv 0(4), u_1 \equiv 1(4) : a_1 = 1, a_2 = 0$ lösen (*).

$u_2 \equiv 0(4), u_1 \equiv 3(4), q \equiv 1(2) : a_1 = 0, a_2 = 1$ lösen (*).

$u_2 \equiv 0(4), u_1 \equiv 3(4), q \equiv 0(2) : (i) \implies a_1^2 \equiv 3(4)$. (*) ist also nicht lösbar.

$u_2 \equiv 2(4)$, $u_1 \equiv 1(4)$, $q \equiv 0(2)$: $a_1 = a_2 = 1$
lösen (*).

$u_2 \equiv 2(4)$, $u_1 \equiv 3(4)$, $q \equiv 0(2)$: (i) $\implies$
 $a_1^2 \equiv 3(4)$. (*) ist nicht lösbar.

(4.9.3.) Seien $d \equiv 1(4)$ und $\tilde{d} \in \mathbb{Z}$ mit $d = 1 + 4\tilde{d}$.

Betrachten wir zunächst die Bedingung, daß u eine

$$\text{Einheit ist : } \left\{ \begin{array}{l} \pm 1 = \text{Norm}(u) \\ = (u_1 + u_2 q \frac{1 + \sqrt{d}}{2})(u_1 + u_2 q \frac{1 - \sqrt{d}}{2}) \\ = u_1^2 + u_1 u_2 q - u_2^2 q^2 \tilde{d}. \end{array} \right\} \quad (*)$$

Das Kriterium (4.8.) wird zu : $[u] \in \text{Bi } D(A_q^d)$

$$\iff \exists a \in A_q^d : a^2 - u \in 4A_q^d$$

$$\iff \exists a_1, a_2 \in \mathbb{Z} : \left\{ \begin{array}{l} \text{(i)} \quad a_1^2 + a_2^2 q^2 \tilde{d} - u_1 \equiv 0(4) \\ \text{(ii)} \quad 2 a_1 a_2 + a_2^2 q - u_2 \equiv 0(4) \end{array} \right\} \quad (**)$$

Damit überlegen wir nun:

$u_2 \equiv 0(4)$, $u_1 \equiv 1(4)$: $a_1 = 1, a_2 = 0$ lösen (**).

$u_2 \equiv 0(4)$, $u_1 \equiv 3(4)$, $q \equiv 0(2)$: (i) $\implies$
 $a_1^2 \equiv 3(4)$; (**) ist nicht lösbar.

$u_2 \equiv 0(4)$, $u_1 \equiv 3(4)$, $q \equiv 1(2)$: (ii) $\implies$
 $a_2^2 \equiv 0(2) \implies a_2 \equiv 0(2)$. In (i) eingesetzt zeigt dies
 $a_1^2 \equiv 3(4)$. (**) ist also nicht lösbar.

$\underline{u_2} \equiv 2(4), \underline{u_1} \equiv 1(4), \underline{q} \equiv 0(4) : a_1 = a_2 = 1$
lösen (**).

$\underline{u_2} \equiv 2(4), \underline{u_1} \equiv 1(4), \underline{q} \equiv 2(4) : \text{Dieser}$
Fall kann nicht auftreten, denn (N) modulo 8 be-
trachtet zeigt $u_1^2 \equiv 1(8), u_2 q \equiv 4(8),$

$u_1 u_2 q \equiv 4(8), u_2^2 q^2 \equiv 0(8) ; \text{ und dies ergibt}$
die Kongruenz $\pm 1 \equiv 1 + 4(8).$

$\underline{u_2} \equiv 2(4), \underline{u_1} \equiv 1(4), \underline{q} \equiv 1(2) : (ii) \implies$
 $a_2 \equiv 0(2) \implies u_2 \equiv 0(4). (**)$ ist nicht lösbar.

$\underline{u_2} \equiv 2(4), \underline{u_1} \equiv 3(4), \underline{q} \equiv 0(2) : (i) \implies$
 $a_1^2 \equiv 3(4). (**)$ ist nicht lösbar.

$\underline{u_2} \equiv 2(4), \underline{u_1} \equiv 3(4), \underline{q} \equiv 1(2) : (ii) \implies$
 $a_2 \equiv 0(2). \text{ In (i) eingesetzt ergibt dies } a_1^2 \equiv 3(4).$
(**) ist nicht lösbar.

$\underline{u_2} \equiv \underline{u_1} \equiv 0(2) : \text{Dieser Fall kann nicht auf-}$
treten. In (N) eingesetzt ergäbe sich ein Widerspruch.
 $\underline{u_2} \equiv 1(2), \underline{q} \equiv 0(2) : (ii) \implies 0 \equiv u_2(2). (**)$
ist nicht lösbar.

Es bleibt also noch der Fall $\underline{u_2} \equiv 1(2), \underline{q} \equiv 1(2)$
zu betrachten. Ist $d \equiv 1(8)$, so kann er nicht auf-
treten, denn : $d \equiv 1(8) \implies \widetilde{d} = 0(2). \text{ (N) modulo 2}$
betrachtet ergibt den Widerspruch $1 \equiv u_1^2 + u_1 \equiv 0(2).$
Für $d \equiv 5(8)$ betrachten wir diesen Fall gesondert.

(4.9.4.) Seien $d \equiv 5(8)$, $d = 1 + 4\tilde{d}$, $\tilde{d} \in \mathbb{Z}$
und $u_2 \equiv 1(2)$, $q \equiv 1(2)$. Dann gilt:

- a.) Ist $u_2 \equiv q(4)$, so liegt $[u]$ genau dann in
 $\text{Bi } D(A_q^d)$, wenn $u_1 \equiv \tilde{d}(4)$ ist.
- b.) Ist $u_2 \not\equiv q(4)$, so liegt $[u]$ genau dann in
 $\text{Bi } D(A_q^d)$, wenn $u_1 \equiv \tilde{d} + 1(4)$ ist.

Bemerkung. In (4.9.4.) untersuchen wir genau die-
jenigen Einheiten von A_q^d , welche nicht in $\mathbb{Z}[\sqrt{d}]$
liegen, denn: $u \notin \mathbb{Z}[\sqrt{d}] \iff u_2 \equiv q \equiv 1(2)$.
Falls $d \equiv 1(8)$ ist, dann gibt es keine solchen
Einheiten in A_q^d , wie wir eben sahen.

Beweis von (4.9.4.). Das Kriterium (**) ist in
diesem Fall äquivalent zu $\left\{ \begin{array}{l} \exists b \in \mathbb{Z} : \quad (i) \ b^2 + \tilde{d} \equiv u_1(4) \\ \quad \quad \quad (ii) \ 2b + q \equiv u_2(4) \end{array} \right\} (+)$.

(**) $\implies$ (+). (ii) $\implies a_2^2 \equiv 1(2) \implies a_2 \equiv 1(2) \implies$
 $2a_2 \equiv 2(4)$, $a_2^2 \equiv 1(4)$. Damit werden die Kongruenzen
zu (i) $a_1^2 + \tilde{d} \equiv u_1(4)$

$$(ii) \ 2a_1 + q \equiv u_2(4) .$$

(**) $\Leftarrow$ (+). Man setze $a_1 := b$ und $a_2 := 1$.

- a.) Sei $u_2 \equiv q(4)$. " $\implies$ " Seien $[u] \in \text{Bi } D(A_q^d)$
und $b \in \mathbb{Z}$ erfülle (+). (ii) $\implies b \equiv 0(2) \implies$
 $u_1 \equiv \tilde{d}(4)$. " $\Leftarrow$ " Ist $u_1 \equiv \tilde{d}(4)$, so ist
 $b = 0$ eine Lösung von (+).

b.) Sei $u_2 \equiv q(4)$. Dies ist gleichwertig mit
 $u_2 - q \equiv 2(4)$. " $\implies$ " Ist b eine Lösung
 von (+), so gilt : (ii) $\implies b \equiv 1(2) \implies$
 $b^2 \equiv 1(4) \implies u_1 \equiv \tilde{d} + 1(4)$. " $\Longleftarrow$ " Ist
 $u_1 \equiv \tilde{d} + 1(4)$, dann ist $b \equiv 1$ eine Lösung
 von (+).

Nun haben wir alle Hilfsmittel bereitgestellt, um die
 GF(2)-Dimensionen der Gruppen $\mathcal{F}(A_q^d)$ zu bestimmen.

(4.11.) Satz.

Es ergeben sich folgende Tabellen von GF(2)-Dimensionen:

a.) Im Fall $d < 0$ erhält man

d, q	$\dim \text{Ke } D$	$\dim \text{Bi } D$	$\dim \mathcal{F}(A_q^d)$
$d \equiv 1(4), q \equiv 2(4)$	1	0	1
$d \equiv 3(4), q \equiv 1(2)$ aber nicht $(d, q) = (-1, 1)$	0	1	1
$d = -1, q = 1$	0	0	0
in allen sonstigen Fällen	0	0	0

b.) Falls $d > 0$ und $d \equiv 2, 3(4)$ ist, dann gilt

d	q	$\xi(\frac{d}{q})_2$	dim Ke D	dim Bi D	dim $\mathcal{F}(A_q^d)$
2(4)	beliebig	0(2)	0	1	1
		1(2)	0	0	0
3(4)	1(2)	0(2)	0	2	2
		1(2)	0	1	1
	0(2)	0(2)	0	1	1
		1(2)	0	0	0

c.) Ist $d > 0$ und $d \equiv 1(4)$, so sind wesentlich mehr Fälle zu unterscheiden. Man erhält

d	q	$\xi(\frac{d}{q})_2$	$\xi(\frac{d}{q})_1$	dimKeD	dimBiD	dim $\mathcal{F}(A_q^d)$
1(4)	0(4)	0(2)	beliebig	0	1	1
		1(2)		0	0	0
	2(4)	0(2)	beliebig	1	1	2
		1(2)		1	0	1
	1(2)	0(4)	beliebig	0	1	1
		2(4)		0	0	0

d	q	$\varepsilon(\frac{d}{q})_2$	$\varepsilon(\frac{d}{q})_1$	dimKeD	dimBiD	$\dim \mathcal{F}(A_q^d)$
5(16)	1(2)	1(2)	2(4)	0	1	1
			0(4)	0	0	0
	1(4)	1(4)	1(4)	0	1	1
			3(4)	0	0	0
			3(4)	0	1	1
			1(4)	0	0	0
	3(4)	3(4)	1(4)	0	1	1
			3(4)	0	0	0
			3(4)	0	1	1
			1(4)	0	0	0
13(16)	1(2)	1(2)	0(4)	0	1	1
			2(4)	0	0	0
	1(4)	1(4)	3(4)	0	1	1
			1(4)	0	0	0
			1(4)	0	1	1
			3(4)	0	0	0
	3(4)	3(4)	3(4)	0	1	1
			1(4)	0	0	0
			1(4)	0	1	1
			3(4)	0	0	0
1(8)	1(2)	1(2)	ist nicht möglich			

Beweis. a.) Die Dimensionen der Kerne entnehmen wir (4.5.). Aus (4.7.) ist bekannt, daß im imaginär-quadratischen Fall die Quadratklassengruppe der Ordnung A_q^d zweielementig ist und aus $[\pm 1]$ besteht, solange $(d, q) \neq (-1, 1)$ ist. Die Dimensionen der Bilder ergeben sich daraus mit (4.10.). Für die Ordnung A_1^{-1} besteht die Quadratklassengruppe aus $[1]$ und $[\sqrt{-1}]$ (4.7.). (4.10.) besagt, daß $\text{Bi } D(A_1^{-1})$ ein-elementig ist.

b.) Die Kerne sind 0, falls $d \equiv 2, 3(4)$ (vgl. 4.5.). Für die Betrachtung der Bilder sei zunächst $d \equiv 2(4)$. Das Ziel von $D(A_q^d)$ ist $\{[\pm 1], [\pm \varepsilon_q^d]\}$ (4.7.). Nach (4.10.) ist $[-1] \notin \text{Bi } D(A_q^d)$. Deshalb ist $\dim \text{Bi } D(A_q^d) \leq 1$, und 1 ist die Dimension genau dann, wenn $[\varepsilon_q^d] \in \text{Bi } D(A_q^d)$ oder $[-\varepsilon_q^d] \in \text{Bi } D(A_q^d)$ ist. Daraufhin betrachten wir nun (4.9.).

Ist $(\varepsilon_q^d)_2 \equiv 1(2)$, dann gilt dies auch für $-(\varepsilon_q^d)_2$;

es ist also weder $[\varepsilon_q^d]$ noch $[-\varepsilon_q^d]$ im Bild von

$D(A_q^d)$. Dagegen ist im Fall $(\varepsilon_q^d)_2 \equiv 0(4)$ stets

$(\varepsilon_q^d)_1 \equiv 1(4)$ oder $-(\varepsilon_q^d)_1 \equiv 1(4)$, und daher ist

$\text{Bi } D(A_q^d)$ stets zweielementig. Analog gilt :

$((\varepsilon_q^d)_2 \equiv 2(4), q \equiv 0(2)) \implies ((\varepsilon_q^d)_1 \equiv 1(4) \text{ oder } -(\varepsilon_q^d)_1 \equiv 1(4))$

$((\varepsilon_q^d)_2 \equiv 2(4), q \equiv 1(2)) \implies ((\varepsilon_q^d)_1 \equiv 3(4) \text{ oder } -(\varepsilon_q^d)_1 \equiv 3(4))$

$-(\varepsilon_q^d)_1 \equiv 3(4)$). Ist also $(\varepsilon_q^d)_2 \equiv 0(2)$, so ist $\text{Bi } D(A_q^d)$ immer zweielementig.

Im Fall $d \equiv 3(4)$ erkennt man auf dieselbe Weise :

$(\varepsilon_q^d)_2 \equiv 1(2) \implies ([\varepsilon_q^d] \notin \text{Bi } D(A_q^d) \text{ und } [-\varepsilon_q^d] \notin \text{Bi } D(A_q^d))$;
 $(\varepsilon_q^d)_2 \equiv 0(2) \implies ([\varepsilon_q^d] \in \text{Bi } D(A_q^d) \text{ oder } [-\varepsilon_q^d] \in \text{Bi } D(A_q^d))$.
 (4.10.) fügt dem hinzu $[-1] \in \text{Bi } D(A_q^d) \iff q \equiv 1(2)$.

c.) Die Dimensionen der Kerne kann man bei (4.5.) ablesen. $[-1] \notin \text{Bi } D(A_q^d)$ (vgl. 4.10.). Es ist also zu untersuchen, unter welchen Voraussetzungen eines der Elemente $[\pm \varepsilon_q^d]$ im Bild von $D(A_q^d)$ liegt.

$q \equiv 0(2)$, $(\varepsilon_q^d)_2 \equiv 0(2)$: Die Normgleichung (N) aus (4.9.3.) zeigt, daß $(\varepsilon_q^d)_1 \equiv 1(2)$ ist. Nach (4.9.) ist deshalb $[\varepsilon_q^d]$ oder $[-\varepsilon_q^d]$ im Bild von D .

$q \equiv 0(2)$, $(\varepsilon_q^d)_2 \equiv 1(2)$: Dann ist auch $-(\varepsilon_q^d)_2 \equiv 1(2)$.

Mit (4.9.) folgt $\dim \text{Bi } D(A_q^d) = 0$.

$q \equiv 1(2)$, $(\varepsilon_q^d)_2 \equiv 0(4)$: (N) $\implies ((\varepsilon_q^d)_1 \equiv 1(4) \text{ oder } -(\varepsilon_q^d)_1 \equiv 1(4)) \implies ([\varepsilon_q^d] \in \text{Bi } D \text{ oder } [-\varepsilon_q^d] \in \text{Bi } D)$.

$q \equiv 1(2)$, $(\varepsilon_q^d)_2 \equiv 2(4)$: Wegen (N) ist $(\varepsilon_q^d)_1 \equiv 1(2)$.

(4.9.) zeigt $[\varepsilon_q^d] \notin \text{Bi } D$. Aber auch $[-\varepsilon_q^d]$

liegt nicht in $\text{Bi } D$, denn $-\varepsilon_q^d$ erfüllt dieselben Kongruenzen.

Es bleibt noch der Fall $q \equiv 1(2)$, $(\varepsilon_q^d)_2 \equiv 1(2)$ zu betrachten. Für $d \equiv 1(8)$ ist er nicht möglich (vgl. 4.9.3.). Die untere Hälfte von (4.11.c) kommt nun durch folgende Überlegung zustande:

$\dim \text{Bi } D(A_q^d)$ ist genau dann 1, wenn $[\varepsilon_q^d]$ oder $[-\varepsilon_q^d]$ in $\text{Bi } D(A_q^d)$ liegt. 1 steht also genau bei denjenigen Quadrupeln $(d, q, (\varepsilon_q^d)_2, (\varepsilon_q^d)_1)$, die selbst oder in Form ihres Gegenstücks $(d, q, -(\varepsilon_q^d)_2, -(\varepsilon_q^d)_1)$ in der Tabelle (4.9.) verzeichnet sind.

(4.12.) Beispiele. Um die zahlreichen Fallunterscheidungen von (4.11.b.) und vor allem von (4.11.c.) zu rechtfertigen, geben wir in derselben Reihenfolge eine Liste von Beispielen an, in denen diese Fälle auftreten. Dazu ziehen wir die Tabelle der Grundeinheiten von Borevič und Šhafarevič ([8] S. 454) heran. Ihr kann man die Grundeinheiten ε_1^d der Hauptordnungen entnehmen. Da für $n \in \mathbb{Z}$ die Ungleichung $-(\varepsilon_1^d)^n < 0$ und für $n \leq 0$ die Ungleichung $(\varepsilon_1^d)^n \leq 1$ gilt, sucht man die Grundeinheiten ε_q^d unter den Potenzen $(\varepsilon_1^d)^n$ mit $n \geq 1$. Und zwar ist ε_q^d die kleinste Potenz von ε_1^d , deren Koeffizient beim Basiselement ω durch q teilbar ist (vgl. [8] S. 151).

d	q	ε_q^d	$(\varepsilon_q^d)_2$
6	1	$5 + 2\sqrt{6}$	2
2	1	$1 + \sqrt{2}$	1
39	1	$25 + 4\sqrt{39}$	4
3	1	$2 + \sqrt{3}$	1
39	2	$25 + 2(2\sqrt{39}) = \varepsilon_1^d$	2
39	4	$25 + 1(4\sqrt{39}) = \varepsilon_1^d$	1

d	q	ε_q^d	$(\varepsilon_q^d)_2$	$(\varepsilon_q^d)_1$
33	4	$19 + 2(4\omega) = \varepsilon_1^{33}$	2	19
17	16	$25 + 1(16\omega) = (\varepsilon_1^{17})^2$	1	25
33	2	$19 + 4(2\omega) = \varepsilon_1^{33}$	4	19
17	2	$3 + 1(2\omega) = \varepsilon_1^{17}$	1	3
33	1	$19 + 8\omega$	8	19
17	1	$3 + 2\omega$	2	3
21	1	$2 + \omega$	1	2
5	1	ω	1	0
5	21	$13 + 1(21\omega) = (\varepsilon_1^5)^8$	1	13
53	1	$3 + \omega$	1	3
69	1	$11 + 3\omega$	3	11
?	1(4)	?	3(4)	1(4)

d	q	ε_q^d	$(\varepsilon_q^d)_2$	$(\varepsilon_q^d)_1$
5	7	$13 + 3(7\omega) = (\varepsilon_1^5)^8$	3	13
?	3(4)	?	3(4)	3(4)
69	3	$11 + 1(3\omega) = \varepsilon_1^{69}$	1	11
?	3(4)	?	1(4)	1(4)
77	1	$4 + \omega$	1	4
29	1	$2 + \omega$	1	2
77	9	$35 + 1(9\omega) = (\varepsilon_1^{77})^2$	1	35
13	1	$1 + \omega$	1	1
93	1	$13 + 3\omega$	3	13
?	1(4)	?	3(4)	3(4)
77	3	$35 + 3(3\omega) = (\varepsilon_1^{77})^2$	3	35
13	11	$43 + 3(11\omega) = (\varepsilon_1^{13})^4$	3	43
93	3	$13 + 1(3\omega) = \varepsilon_1^{93}$	1	13
?	3(4)	?	1(4)	3(4)

Die Fragezeichen in der zweiten Tabelle signalisieren Fälle, für die wir kein Beispiel angeben können, von denen wir aber auch nicht zeigen können, daß sie nicht vorkommen. Doch genügt auch diese unvollständige Tabelle zur Rechtfertigung der Fallunterscheidungen in (4.11.c.).

§ 2 Die Gruppe der quadratischen Erweiterung
mit Normalbasis von A_q^d

C. Small hat am Ende von [39] das Beispiel $\mathcal{N}(A_1^2) = 0$ angegeben und für die Hauptordnungen reell-quadratischer Zahlkörper die Vermutung geäußert

$$\mathcal{N}(A_1^d) \begin{cases} = 0, & \text{falls } d \equiv 2(4) \\ \neq 0, & \text{falls } d \equiv 3(4) \end{cases}.$$

Daß diese Vermutung etwas voreilig war, hat bereits Théron [40] gezeigt. Er bestimmt in dieser Arbeit die Gruppen $\mathcal{N}(A_1^d)$ unabhängig von seinen Überlegungen zur Bestimmung von $\mathcal{F}(A_1^d)$ in [41].

Wir haben aus Kapitel 3 eine andere Möglichkeit um die Struktur der Gruppen $\mathcal{N}(A_q^d)$ zu bestimmen. (3.36.) gibt uns dazu die exakte Folge

$$0 \longrightarrow \mathcal{N}(A_q^d) \longrightarrow \mathcal{F}(A_q^d) \xrightarrow{P(A_q^d)} \frac{U(A_q^d/2A_q^d)}{\text{Bi}(U\pi_2)(A_q^d)}.$$

d sei weiterhin eine ganzrationale quadratfreie Zahl $\neq 1$, und q sei eine natürliche Zahl ≥ 1 .

Zunächst betrachten wir das Ziel von P . A_q^d ist ein freier $\mathbb{Z}$ -Modul mit der Basis $\{1, q\omega\}$. Deshalb ist

$A_q^d/2A_q^d$ ein freier $\mathbb{Z}/2\mathbb{Z}$ -Modul mit der Basis $\{\overline{1}, \overline{q\omega}\}^+)$. $A_q^d/2A_q^d = \{\overline{0}, \overline{1}, \overline{q\omega}, \overline{1 + q\omega}\}$.

(4.13.) Proposition. Ist $a \in A_q^d$ und $\overline{a} \in U(A_q^d/2A_q^d)$, so ist $N(a) \equiv 1(2)$.

Beweis. Der nicht-triviale Automorphismus von $\mathbb{Q}(\sqrt{d})$ sei mit σ bezeichnet. Ist $\overline{a} \in U(A_q^d/2A_q^d)$, so gibt es $b, c \in A_q^d$ mit $ab = 1 + 2c$. Dafür gilt $N(a)N(b) = (ab)\sigma(ab) = (1 + 2c)\sigma(1 + 2c) = 1 + 2c + 2\sigma(c) + 4c\sigma(c) = 1 + 2\text{tr}(c) + 4N(c)$.

Da $\text{tr}(c), N(c) \in \mathbb{Z}$ sind, ist $N(a) \equiv 1(2)$.

(4.14.) Proposition. $U(A_q^d/2A_q^d)$ hat in Abhängigkeit von d und q folgende Gestalt

d	q	$U(A_q^d/2A_q^d)$
2(4)	beliebig	$\{\overline{1}, \overline{1 + q\omega}\}$
3(4)	0(2)	$\{\overline{1}, \overline{1 + q\omega}\}$
3(4)	1(2)	$\{\overline{1}, \overline{q\omega}\}$
1(4)	0(2)	$\{\overline{1}, \overline{1 + q\omega}\}$
1(8)	1(2)	$\{\overline{1}\}$
5(8)	1(2)	$\{\overline{1}, \overline{q\omega}, \overline{1 + q\omega}\}$

⁺) Wie in Kapitel 3 bezeichnen wir Restklassen nach dem von 2 erzeugten Ideal mit einem Querstrich.

Beweis. Sei $a_1 + a_2 q \omega \in A_q^d$ mit $a_i \in \mathbb{Z}$. Für

$d \equiv 2, 3(4)$ ist $N(a_1 + a_2 q \omega) = a_1^2 - a_2^2 q^2 d$. Ist

$d \equiv 1(4)$ und $d = 1 + 4\tilde{d}$, $\tilde{d} \in \mathbb{Z}$, so ist $N(a_1 + a_2 q \omega) =$
 $= a_1^2 + a_1 a_2 q - a_2^2 q^2 \tilde{d}$ (vgl. Beweis von 4.9.).

$d \equiv 2(4)$: $N(q\omega) \equiv 0(2) \implies \overline{q\omega} \notin U(A_q^d/2A_q^d)$ (4.13.) ;

$$\overline{1 + q\omega}^2 = \overline{(1 + q^2 d) + 2q\omega} = \overline{1}.$$

$d \equiv 3(4)$, $q \equiv 0(2)$: $N(q\omega) \equiv 0(2)$ und $\overline{1 + q\omega}^2 = \overline{1}$.

$d \equiv 3(4)$, $q \equiv 1(2)$: $N(1 + q\omega) \equiv 0(2)$ und $\overline{q\omega}^2 = \overline{q^2 d} = \overline{1}$.

$d \equiv 1(4)$, $q \equiv 0(2)$: $N(q\omega) = -q^2 \tilde{d} \equiv 0(2)$ und

$$\overline{1 + q\omega}^2 = \overline{1 + 2q\omega + q^2(\omega + \tilde{d})} = \overline{1 + q^2 \tilde{d} + (2+q)q\omega} = \overline{1}.$$

$d \equiv 1(8)$, $q \equiv 1(2)$: In diesem Fall ist $\tilde{d} \equiv 0(2)$.

$$N(q\omega) = -q^2 \tilde{d} \equiv 0(2) \text{ und}$$

$$N(1 + q\omega) = 1 + q - q^2 \tilde{d} \equiv 0(2).$$

$d \equiv 5(8)$, $q \equiv 1(2)$: $\overline{1 + q\omega} \overline{q\omega} = \overline{q^2 \tilde{d} + (q+1)q\omega} = \overline{1}$, denn hier ist $\tilde{d} \equiv 1(2)$.

(4.15.) Satz. a.) Für alle Ordnungen imaginär-quadratischer Zahlkörper ($d < 0$) ist $\mathcal{N}(A_q^d) = 0$.

b.) Ist $d > 0$, so ist $\mathcal{N}(A_q^d) \xrightarrow{\neq} \mathcal{F}(A_q^d)$ genau für folgende Tripel $(d, q, (\mathcal{E}_q^d)_2)$ eine echte Untergruppe :

d	q	$(\mathcal{E}_q^d)_2$	$\dim \mathcal{N}(A_q^d)$	$\dim \mathcal{F}(A_q^d)$
2(4)	beliebig	2(4)	0	1
3(4)	0(2)	2(4)	0	1
3(4)	1(2)	0(2)	1	2
1(4)	0(4)	2(4)	0	1
1(4)	2(4)	0(2)	1	2

In allen anderen Fällen ist $\mathcal{N}(A_q^d) = \mathcal{F}(A_q^d)$.

Beweis. a.) In diesem Fall genügt es, das Anfangsstück der Folge (3.36.) zu betrachten.

$$0 \longrightarrow \text{Ip}(A_q^d) \longrightarrow U_2(A_q^d) \xrightarrow{(\quad)^2} U_4(A_q^d) \longrightarrow \mathcal{N}(A_q^d) \longrightarrow 0$$

ist eine exakte Folge. Im Beweis von (4.7.a.) haben wir uns überlegt, wie die Gruppen $U(A_q^d)$, $d < 0$ aussehen. Daraus erkennt man, daß $U_4(A_q^d) = \{1\}$ ist.

b.) Sei zunächst $d \equiv 2(4)$. Nach (4.14.) ist dann

$U(A_q^d/2A_q^d) = \{\bar{1}, \overline{1 + q\omega}\}$. Man macht sich schnell klar, daß gilt

$$\text{Bi}(U\pi_2)(A_q^d) = \left\{ \begin{array}{ll} \{\bar{1}\}, & \text{falls } (\mathcal{E}_q^d)_2 \equiv 0(2) \\ \{\bar{1}, \overline{1 + q\omega}\}, & \text{falls } (\mathcal{E}_q^d)_2 \equiv 1(2) \end{array} \right\}.$$

Im Fall $(\mathcal{E}_q^d)_2 \equiv 1(2)$ ist nichts zu zeigen. Sei also

$(\mathcal{E}_q^d)_2 \equiv 0(2)$. Dann ist $\mathcal{F}(A_q^d)$ zweielementig und ent-

hält neben dem trivialen Element ein Element der Form

$[\mathcal{E}_q^d, \bar{a}]$ oder eines der Form $[-\mathcal{E}_q^d, \bar{a}]$, mit $a \in A_q^d$

(4.11.). Für dieses $a \in A_q^d$ gilt also $a^2 - u \in 4A_q^d$, wobei $u = +\varepsilon_q^d$ oder $u = -\varepsilon_q^d$ ist. Wie in (4.9.1.) erhält man also Kongruenzen

$$\left\{ \begin{array}{l} \text{(i)} \quad a_1^2 - u_1 + a_2^2 q^2 d \equiv 0(4) \\ \text{(ii)} \quad 2a_1 a_2 - u_2 \equiv 0(4) \end{array} \right\}.$$

Da $(\varepsilon_q^d)_1 \equiv -(\varepsilon_q^d)_1 \equiv 1(2)$ gilt, ist $a_1 \equiv 1(2)$.

Ist $(\varepsilon_q^d)_2 \equiv 0(4)$, so ist auch $-(\varepsilon_q^d)_2 \equiv 0(4)$. (ii)

zeigt daher $a_2 \equiv 0(2)$. In diesem Fall ist also

$\text{Bi } P(A_q^d) = \{ [\bar{1}] \}$. Ist andererseits $(\varepsilon_q^d)_2 \equiv 2(4)$,

dann ist auch $-(\varepsilon_q^d)_2 \equiv 2(4)$. Daher ist in diesem

Fall $a_2 \equiv 1(2)$, $\text{Bi } P(A_q^d)$ ist zweielementig und

$$\text{Ke } P(A_q^d) = \mathcal{N}(A_q^d) = 0.$$

Sei nun $d \equiv 3(4)$, $q \equiv 0(2)$. Ist $(\varepsilon_q^d)_2 \equiv 1(2)$, so

ist $\mathcal{F}(A_q^d) = 0$. Dieser Fall ist also klar. Ist $(\varepsilon_q^d)_2$

$\equiv 0(2)$, so ist $\mathcal{F}(A_q^d)$ zweielementig. Ein Blick auf

(4.14.) zeigt, daß $U(A_q^d/2A_q^d) = \{ \bar{1}, \overline{1 + q\omega} \}$ ist.

Dieselben Überlegungen wie im Fall $d \equiv 2(4)$,

$(\varepsilon_q^d)_2 \equiv 0(2)$ zeigen die Behauptung.

Schließlich seien $d \equiv 3(4)$, $q \equiv 1(2)$. Nach (4.14.) ist

$U(A_q^d/2A_q^d) = \{ \bar{1}, \overline{q\omega} \}$. Wie man sofort sieht, ist

$$\text{Bi}(U\pi_2)(A_q^d) = \left\{ \begin{array}{l} \{ \bar{1} \}, \text{ falls } (\varepsilon_q^d)_2 \equiv 0(2) \\ \{ \bar{1}, \overline{q\omega} \}, \text{ falls } (\varepsilon_q^d)_2 \equiv 1(2) \end{array} \right\}.$$

Im Fall $(\varepsilon_q^d)_2 \equiv 1(2)$ ist daher $P(A_q^d)$ die Nullabbildung.

Also ist $\mathcal{N}(A_q^d) = \text{Ke } P(A_q^d) = \mathcal{F}(A_q^d)$. Ist $(\varepsilon_q^d)_2 \equiv 0(2)$,

so ist $[-1] \in \text{Bi } D(A_q^d)$ (vgl. 4.10.). Es gibt also ein $a \in A_q^d$ mit $-1 - a^2 \in 4A_q^d$. Für dieses a gilt dann

$$[-1, \bar{a}] \in \mathcal{F}(A_q^d) \quad \text{und} \quad [\bar{a}] \in \text{Bi } P(A_q^d).$$

$$1 + a^2 \in 4A_q^d \implies \left\{ \begin{array}{l} \text{(i)} \quad a_1^2 + a_2^2 q^2 d + 1 \equiv 0(4) \\ \text{(ii)} \quad 2a_1 a_2 \equiv 0(4) \end{array} \right\}.$$

Wäre $a_2 \equiv 0(2)$, so hätte (i) die Gestalt $a_1^2 \equiv 3(4)$.

Da dies nicht möglich ist, ist $a_2 \equiv 1(2)$ und $a_1 \equiv 0(2)$.

Deshalb ist $P[-1, \bar{a}] = [\bar{a}] = [\overline{q\omega}]$; $\dim \text{Bi } P(A_q^d) = 1$.

Der Fall $d > 0$, $d \equiv 1(4)$ ist erwartungsgemäß etwas mühsamer. $U(A_q^d/2A_q^d)$ hat dann die Ordnung 1, 2 oder 3.

Ist $(\varepsilon_q^d)_2 \equiv 1(2)$, so gilt: $\pi_2(\varepsilon_q^d) \neq \pi_2(1) \implies$

$$\text{Bi}(U\pi_2)(A_q^d) = U(A_q^d/2A_q^d) \implies P(A_q^d) = 0$$

$$\implies \mathcal{N}(A_q^d) = \text{Ke } P(A_q^d) = \mathcal{F}(A_q^d).$$

Sei nun $(\varepsilon_q^d)_2 \equiv 0(2)$. Dann gilt: $\pi_2(\varepsilon_q^d) = \pi_2(1)$

$$\implies \text{Bi}(U\pi_2)(A_q^d) = \{\bar{1}\} \implies$$

$$\frac{U(A_q^d/2A_q^d)}{\text{Bi}(U\pi_2)(A_q^d)} = \begin{cases} \{[\bar{1}]\}, & \text{falls } d \equiv 1(8), q \equiv 1(2) \\ \{[\bar{1}], [\overline{1+q\omega}]\}, & \text{falls } d \equiv 1(4), q \equiv 0(2) \\ \{[\bar{1}], [\overline{q\omega}], [\overline{1+q\omega}]\}, & \text{falls } d \equiv 5(8), q \equiv 1(2) \end{cases}$$

Wir unterscheiden wieder einige Fälle.

$$q \equiv 1(2), (\varepsilon_q^d)_2 \equiv 2(4) : \mathcal{F}(A_q^d) = 0 \implies \mathcal{N}(A_q^d) = 0.$$

$$q \equiv 1(2), (\varepsilon_q^d)_2 \equiv 0(4) : \mathcal{F}(A_q^d) \simeq \mathbb{Z}/2\mathbb{Z}. \text{ Ist } d \equiv 1(8),$$

so ist das Ziel von $P(A_q^d)$ trivial, und deshalb ist

$$\mathcal{N}(A_q^d) = \mathcal{F}(A_q^d). \text{ Ist } d \equiv 5(8), \text{ so ist das Ziel von}$$

P isomorph zu $\mathbb{Z}/3\mathbb{Z}$. Auch dafür ist P also die Nullabbildung, und es ist $\mathcal{N}(A_q^d) = \mathcal{F}(A_q^d)$.

Es bleibt also der Fall $q \equiv 0(2), (\varepsilon_q^d)_2 \equiv 0(2)$ zu betrachten. In diesem Fall ist das Ziel von $P(A_q^d)$ von der Gestalt $\{[\overline{1}], [\overline{1+q\omega}]\}$. Im Beweis von (4.11.) haben wir überlegt, daß $\text{Bi } D(A_q^d)$ zweielementig ist.

Das nicht-triviale Element

$$\text{in Bi } D(A_q^d) \text{ ist } \left\{ \begin{array}{l} [\varepsilon_q^d], \text{ falls } (\varepsilon_q^d)_1 \equiv 1(4) \\ [-\varepsilon_q^d], \text{ falls } (\varepsilon_q^d)_1 \equiv 3(4) \end{array} \right\}.$$

Es gibt also $a_1, a_2 \in \mathbb{Z}$, so daß

$$(a_1 + a_2 q \omega)^2 + \varepsilon_q^d \in 4A_q^d \text{ ist. Mit der Bezeichnung}$$

$d = 1 + 4 \tilde{d}$ ist dies äquivalent zu

$$\left\{ \begin{array}{l} \text{(i)} \quad a_1^2 + a_2^2 q^2 \tilde{d} + (\varepsilon_q^d)_1 \equiv 0(4) \\ \text{(ii)} \quad 2a_1 a_2 + a_2^2 q + (\varepsilon_q^d)_2 \equiv 0(4) \end{array} \right\}.$$

Das Minuszeichen tritt bei $+$ genau dann ein, wenn

$$(\varepsilon_q^d)_1 \equiv 1(4) \text{ ist. Da außerdem } (\varepsilon_q^d)_2 \equiv -(\varepsilon_q^d)_2 \pmod{4}$$

ist, erhalten wir

$$\left\{ \begin{array}{l} \text{(i)} \quad a_1^2 \equiv 1(4) \\ \text{(ii)} \quad 2a_1a_2 + a_2^2 q - (\varepsilon_q^d)_2 \equiv 0(4) \end{array} \right\}.$$

$q \equiv 0(4)$, $(\varepsilon_q^d)_2 \equiv 0(4)$: $\mathcal{F}(A_q^d) = \text{Bi } D(A_q^d)$. P schickt das nicht-triviale Element auf $[\bar{a}]$, wobei a den Kongruenzen (i) und (ii) genügt. (ii) $\implies a_2 \equiv 0(2) \implies [\bar{a}] = [\bar{1}] \implies P(A_q^d) = 0 \implies \mathcal{N}(A_q^d) = \mathcal{F}(A_q^d)$.

$q \equiv 0(4)$, $(\varepsilon_q^d)_2 \equiv 2(4)$: Wie für $(\varepsilon_q^d)_2 \equiv 0(4)$ ist $\mathcal{F}(A_q^d)$ zweielementig, und es gilt $\text{Bi } P(A_q^d) = \{[\bar{1}], [\bar{a}]\}$, wobei für a die Kongruenzen (i) und (ii) gelten. Doch nun folgt : (ii) $\implies a_2 \equiv 1(2) \implies [\bar{a}] = [\overline{1 + q\omega}] \implies \mathcal{N}(A_q^d) = \text{Ke } P(A_q^d) = 0$.

$q \equiv 2(4)$, $(\varepsilon_q^d)_2 \equiv 0(4)$: $\dim \mathcal{F}(A_q^d) = 2$;

$\text{Bi } P(A_q^d) \subseteq \{[\bar{1}], [\overline{1 + q\omega}]\}$. Man prüft leicht nach,

daß $(1 + q\omega)^2 \mp \varepsilon_q^d \in 4A_q^d$ ist, wobei das Minuszeichen im Fall $(\varepsilon_q^d)_1 \equiv 1(4)$ und das Pluszeichen im Fall $(\varepsilon_q^d)_1 \equiv 3(4)$ zu nehmen ist. Deshalb gilt

$$[\mp \varepsilon_q^d, \overline{1 + q\omega}] \in \mathcal{F}(A_q^d), \dim \text{Bi } P(A_q^d) = 1,$$

$$\dim \text{Ke } P(A_q^d) = 1.$$

$q \equiv 2(4)$, $(\varepsilon_q^d)_2 \equiv 2(4)$: Dieser Fall ist nicht möglich,

denn: $\varepsilon_q^d \in U(A_q^d) \implies$

$$\pm 1 = (\varepsilon_q^d)_1^2 + (\varepsilon_q^d)_1 (\varepsilon_q^d)_2 q - (\varepsilon_q^d)_2^2 q^2 \sim (4.9.3.)$$

$$\implies (\varepsilon_q^d)_1^2 \equiv \pm 1(4)$$

$$\implies N(\varepsilon_q^d) = 1 \text{ und } (\varepsilon_q^d)_1 \equiv 1(2)$$

$$\implies (\varepsilon_q^d)_1^2 \equiv 1(8), (\varepsilon_q^d)_1 (\varepsilon_q^d)_2 \equiv 4(8), (\varepsilon_q^d)_{2q}^{2q} \equiv 0(8)$$

$$\implies 1 \equiv 5(8).$$

(4.16.) Bemerkungen. a.) Für die Hauptordnungen A_1^d , $d < 0$ hat C. Small (4.15.a.) als Beispiel aufgeführt (vgl. [38] S. 104).

b.) Aus (4.15.b.) folgt für die Hauptordnungen A_1^d , $d > 0$, $d \equiv 3(4)$: $\dim \mathcal{N}(A_1^d) = 1$. Smalls Vermutung ist also teilweise richtig (vgl. Théron [40] Théorème 1). Es folgt aber auch, daß der andere Teil der Vermutung falsch ist: Für $d = 14$ ist $\varepsilon_1^d = 15 + 4\sqrt{14}$ ([8] S. 454), $\mathcal{N}(A_1^{14})$ ist also $\neq 0$ (vgl. Théron [40] Remarque 1).

c.) Im Fall $d \equiv 1(4)$, $d > 0$ gibt Théron ([40] Th. 1) ein Kriterium für " $\dim \mathcal{N}(A_1^d) = 1$ " an, welches die Grundeinheit von $\mathbb{Z}[\sqrt{d}] = A_2^d$ benützt. Die gängigen Tabellen geben aber nur die Grundeinheiten von A_1^d an (vgl. Ince, E.L.: Math. Tables IV, Cycles of reduced ideals in quadratic fields. Univ. Press Cambridge, 1968). So ist es i. a. bequemer (4.15.) und (4.11.) zu benutzen.

(4.17.) Beispiele. Nach (4.15.) sind wir natürlich an Beispielen interessiert, welche zeigen, daß die Be-

dingung " $(\varepsilon_q^d)_2 \equiv 2(4)$ " nicht einfach durch

" $(\varepsilon_q^d)_2 \equiv 0(2)$ " ersetzt werden kann. Dazu ergänzen wir (4.12.) durch

d	q	ε_q^d	$(\varepsilon_q^d)_2$	$(\varepsilon_q^d)_1$
14	1	$15 + 4\omega$	4	15
7	2	$127 + 24(2\omega) = (\varepsilon_1^7)^2$	24	127
17	4	$25 + 4(4\omega) = (\varepsilon_1^{17})^2$	1	25

Anhang: Bemerkungen zu Thérond [41]

In der Einleitung wurde erwähnt, daß der Anstoß zur vorliegenden Arbeit von den Fehlern in [41] ausging. Dies möchte ich nun nicht einfach damit abtun, daß ich die hier erzielten Resultate neben diejenigen von Thérond stelle.

Hier soll diskutiert werden, welche der Aussagen Théronds falsch sind und wo der jeweilige Fehler steckt.

(4.18.) Bezeichnungen. Für einen kommutativen Ring R

sei $\tilde{\mathcal{K}}(R) := \{(a, b) \mid a, b \in R, a^2 + 4b \in U(R)\}$, und

$\sim_R$ sei folgende Äquivalenzrelation auf $\tilde{\mathcal{K}}(R)$

$$(a, b) \sim_R (a', b') : \Longleftrightarrow \left\{ \begin{array}{l} \exists \alpha \in U(R), \beta \in R : \\ a' = \alpha(a - 2\beta) \\ b' = \alpha^2(\beta a + b - \beta^2) \end{array} \right\}.$$

$\mathcal{K}(R) := \widetilde{\mathcal{K}}(R) / \sim_R$ ist dann dieselbe Menge, wie wir sie in (3.17.) betrachtet haben. Sie ist Kitamuras Beschreibung der Gruppe der freien quadratischen Erweiterungen von R (vgl. 3.18.).

Im folgenden sei stets $d > 0$, quadratfrei. A^d sei die Hauptordnung in $\mathbb{Q}(\sqrt{d})$, und $\varepsilon^d = (\varepsilon^d)_1 + (\varepsilon^d)_2 \omega$ sei die Grundeinheit von A^d .

(4.19.). In ([41] Lemma 1) und im zugehörigen Korollar wird behauptet: "Ist $\varepsilon^d \in \mathbb{Z}[\sqrt{d}]$, so sind $\mathcal{K}(A^d) \simeq \mathcal{K}(\mathbb{Z}[\sqrt{d}])$ isomorph. Insbesondere sind diese Gruppen isomorph, falls $d \equiv 1(8)$." Diese Aussage ist falsch.

Gegenbeispiel. Für $d = 17$ ist $\varepsilon_1^{17} = 3 + 2\omega = 4 + \sqrt{17} \in \mathbb{Z}[\sqrt{17}] = A_2^{17}$ ([8] S. 454). Deshalb ist $\varepsilon_2^{17} = 3 + 1(2\omega)$. Nach (4.11.) ist daher $\mathcal{F}(A_1^{17}) = 0$, aber $\mathcal{F}(A_2^{17}) \simeq \mathbb{Z}/2\mathbb{Z}$.

Der Fehler. Es wird nur gezeigt $\widetilde{\mathcal{K}}(A^d) = \widetilde{\mathcal{K}}(\mathbb{Z}[\sqrt{d}])$. Aber auch die Äquivalenzrelation auf $\widetilde{\mathcal{K}}(R)$ ist vom Ring R abhängig, wie folgendes Beispiel zeigt: Sei $d \equiv 1(8)$, $d = 1 + 4\tilde{d}$. Dann sind $(1, 0)$ und $(1 - 2\omega, -\tilde{d})$ Elemente von $\widetilde{\mathcal{K}}(\mathbb{Z}[\sqrt{d}]) \subseteq \widetilde{\mathcal{K}}(A^d)$, denn $(1 - 2\omega)^2 - 4\tilde{d} = 1 - 4\omega + 4\omega^2 - 4\tilde{d} = 1$. Außerdem sind sie bezüglich der Äquivalenzrelation zum Ring A^d äquivalent. $(1 - 2\omega, -\tilde{d}) \sim_{A^d} (1, 0)$, denn für $1 \in U(A^d)$, $\omega \in A^d$ erhält man

$$(i) \quad 1 - 2\omega = 1 (1 - 2\omega)$$

$$(ii) \quad 1^2 (\omega + 0 - \omega^2) = -\tilde{d}.$$

Jedoch gibt es kein Paar $\alpha \in U(\mathbb{Z}[\sqrt{d}])$,

$\beta \in \mathbb{Z}[\sqrt{d}]$, für welches gilt

$$(i) \quad 1 - 2\omega = \alpha(1 - 2\beta)$$

$$(ii) \quad -\tilde{d} = \alpha^2(\beta - \beta^2).$$

Um die letzte Behauptung zu zeigen, nehmen wir an,

(i) und (ii) würden gelten. Quadrieren von (i) und

Einsetzen von (ii) ergäbe dann

$$1 - 4\omega + 4\omega^2 = \alpha^2 - 4\alpha^2(\beta - \beta^2) = \alpha^2 + 4\tilde{d} \\ \implies 1 + 4\tilde{d} = \alpha^2 + 4\tilde{d} \implies \alpha^2 = 1.$$

Wäre aber $\alpha = 1$, so erhielte man aus (i), daß

$\beta = \omega \in \mathbb{Z}[\sqrt{d}]$ ist. Für $\alpha = -1$ wäre analog $2\beta = 2(1 - \omega)$;

also $\beta = 1 - \omega \in \mathbb{Z}[\sqrt{d}]$. In beiden Fällen ergäbe sich also ein Widerspruch.

(4.20.). In [41] Proposition 1 wird behauptet :

" $D(\mathbb{Z}[\sqrt{d}])$ ist injektiv". (Die Implikationen

$(a) \iff (b) \implies (c)$ sind trivial. $(c) \implies (b)$ bedeutet gerade, daß D injektiv ist.)

Diese Aussage ist falsch.

Gegenbeispiel. Für $d \equiv 1(4)$ ist $D(\mathbb{Z}[\sqrt{d}]) = D(A_2^d)$ nicht injektiv (vgl. 4.6.).

Man sieht dies auch direkt, wenn man ein konkretes Beispiel betrachtet.

Seien $d = 5$ und $a := \sqrt{5}$, $b := -1$, $a' := 1$,
 $b' := 0$. Dann gilt $a^2 + 4b = 1 = a'^2 + 4b'$. Also
sind $[a, b], [a', b'] \in \mathcal{K}(\mathbb{Z}[\sqrt{5}])$, und es gilt
 $D[a, b] = D[a', b']$.

Nehmen wir nun an $[a, b] = [a', b']$. Dann existieren
 $u \in U(\mathbb{Z}[\sqrt{5}])$, $v \in \mathbb{Z}[\sqrt{5}]$, so daß gilt

$$(i) \quad 1 = u(\sqrt{5} - 2v)$$

$$(ii) \quad 0 = u^2(v\sqrt{5} - 1 - v^2) \quad .$$

Wäre $[a, b] = [a', b']$, dann hätte das Polynom

$x^2 - \sqrt{5}x + 1$ also in $\mathbb{C}$ neben den Lösungen

$\frac{\sqrt{5} \pm 1}{2}$ noch eine dritte Lösung v , welche in $\mathbb{Z}[\sqrt{5}]$
liegt.

Der Fehler. Es wird folgende falsche Implikation
benutzt: " $\forall a, a' \in \mathbb{Z}[\sqrt{d}], u \in U(\mathbb{Z}[\sqrt{d}])$:

$$a^2 \equiv (ua')^2 \pmod{4\mathbb{Z}[\sqrt{d}]} \implies$$

$$a \equiv ua' \pmod{2\mathbb{Z}[\sqrt{d}]} \quad .$$

Wählt man z.B. d, a, a' wie oben und $u = 1$, so
hat man ein Gegenbeispiel zu dieser Implikation.

Proposition 2 von [41] besagt: " $D(A_1^d)$ ist injektiv
für alle $d > 0$ ". Dies ist richtig (vgl. 4.6.). Im Be-
weis davon heben sich die Fehler von Lemma 1 und
Proposition 1 auf. Lemma 3 von [41] ist die bis
dahin einzige Aussage, für welche ein richtiger Be-
weis angegeben wird. Es besagt: " $[-1] \in \text{Bi } D(A_1^d)$ "

$\iff d \equiv 3(4)"$ (vgl. 4.10.).

(4.21.). Théorème 1 von [41] lautet : "Sei

$\varepsilon^d = x^d + y^d \sqrt{d}$ mit $x^d, y^d \in \mathbb{Z}$ die Grundeinheit von A_1^d , dann gilt

(a) Ist $\varepsilon^d \notin \mathbb{Z}[\sqrt{d}]$, so sind $\mathcal{F}(A^d) \simeq \mathbb{Z}/2\mathbb{Z}$ isomorph.

(b) Ist $\varepsilon^d \in \mathbb{Z}[\sqrt{d}]$, so gibt es Isomorphismen

$\mathcal{F}(A_1^d) \simeq \mathbb{Z}/2\mathbb{Z}$ oder $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, falls $d \equiv 3(4)$

$\mathcal{F}(A_1^d) \simeq 0$ oder $\mathbb{Z}/2\mathbb{Z}$, falls $d \equiv 1, 2(4)$. Die

größere der beiden Gruppen tritt jeweils dann

auf, wenn $y^d \equiv 0(2)$."

Teil (b) von Théorème 1 ist richtig (vgl. 4.11.).

Der Beweis davon ist natürlich falsch, da die falsch

bewiesene Proposition 2 entscheidend eingeht. Auch

hier ergibt sich die richtige Aussage nur deshalb,

weil sich die Fehler von Lemma 1 und Proposition 1

aufheben.

Teil (a) von Théorème 1 ist jedoch falsch.

Der Fehler. Thérond zeigt nur : höchstens eine der beiden Klassen $[\varepsilon^d]$, $[-\varepsilon^d]$ liegt im Bild von $D(A^d)$.

Der Satz "La réciproque est claire" soll vermutlich

besagen, daß mindestens eine dieser beiden Klassen

im Bild von D liegt. Doch dies ist eben gar nicht

"claire", wie folgendes Gegenbeispiel zeigt.

Gegenbeispiel. Für $d = 5$ ist die Grundeinheit ε_1^5 der Hauptordnung gleich ω . Wir wenden Satz (4.11.) an und sehen: $d \equiv 5(16)$, $q \equiv 1(4)$, $(\varepsilon_1^5)_2 \equiv 1(4)$, $(\varepsilon_1^5)_1 \equiv 0(4) \implies \mathcal{F}(A_1^5) = 0$. Daher ist auch die Behauptung Théronds ([40] S. 121) " $\mathcal{N}(A_1^5) \neq \mathcal{F}(A_1^5)$ " falsch.

Wir wollen noch zeigen, wie dies aus dem Ansatz von Théronnd folgt.

Direkter Beweis des Gegenbeispiels. Wir wissen bereits, daß $D(A_1^5)$ ein Monomorphismus ist und daß $[-1] \notin \text{BiD}(A_1^5)$ ist. Théronnd zeigt mit der Bezeichnung $\varepsilon_1^5 = \frac{\eta'}{2} + \frac{\xi'}{2}\sqrt{5}$: Von den beiden Klassen $[\varepsilon_1^5]$, $[-\varepsilon_1^5]$ liegt höchstens diejenige im Bild von $D(A_1^5)$, für welche $\pm \eta' \equiv 3(4)$ ist. Also ist $[+\varepsilon_1^5] \notin \text{BiD}(A_1^5)$, denn $\varepsilon_1^5 = \frac{1}{2} + \frac{1}{2}\sqrt{5}$.

Wir zeigen nun, daß auch die Annahme $[-\varepsilon_1^5] \in \text{BiD}(A_1^5)$ zu einem Widerspruch führt. Dabei verwenden wir Théronnds Bezeichnungsweise.

Seien $a = \frac{\alpha'}{2} + \frac{\beta'}{2}\sqrt{5}$, $b = \frac{\alpha''}{2} + \frac{\beta''}{2}\sqrt{5} \in A^5$, d.h. für $\alpha', \beta', \alpha'', \beta'' \in \mathbb{Z}$ soll $\alpha' \equiv \beta' (2)$ und $\alpha'' \equiv \beta'' (2)$ gelten. Sei $a^2 + 4b = -\varepsilon_1^5$.

Daraus folgt durch Einsetzen

$$\frac{1}{4} (\alpha'^2 + 2\alpha'\beta'\sqrt{5} + 5\beta'^2) + 2\alpha'' + 2\beta''\sqrt{5} = -\frac{1}{2} - \frac{1}{2}\sqrt{5}$$

$$\implies \left\{ \begin{array}{l} \text{(i)} \quad -\frac{1}{2} = \frac{1}{4} (\alpha'^2 + 5\beta'^2 + 8\alpha'') \\ \text{(ii)} \quad -\frac{1}{2} = \frac{1}{4} (2\alpha'\beta' + 8\beta'') \end{array} \right\}$$

$$\Rightarrow \left\{ \begin{array}{l} \text{(i)} \quad -2 = \alpha'^2 + 5\beta'^2 + 8\alpha'' \\ \text{(ii)} \quad -1 = \alpha'\beta' + 4\beta'' \end{array} \right\}.$$

(ii) zeigt $\alpha'\beta' \equiv 1(2)$, also ist $\alpha' \equiv \beta' \equiv 1(2)$.

Nun sind zwei Fälle zu unterscheiden.

$\alpha'' \equiv \beta'' \equiv 0(2)$: Aus (ii) folgt $\alpha'\beta' \equiv 7(8)$. Es gibt also die Möglichkeiten ($\alpha' \equiv \pm 1(8)$ und $\beta' \equiv \mp 1(8)$) oder ($\alpha' \equiv \pm 3(8)$ und $\beta' \equiv \mp 3(8)$). Im ersten Fall ist $\alpha'^2 \equiv \beta'^2 \equiv 1(16)$, im anderen Fall ist $\alpha'^2 \equiv \beta'^2 \equiv 9(16)$. In beiden Fällen wird (i) zu $-2 \equiv 6(16)$.

$\alpha'' \equiv \beta'' \equiv 1(2)$: Es ist $4\beta'' \equiv 4(8)$. (ii) zeigt daher $3 \equiv \alpha'\beta'(8)$

$\Rightarrow (\alpha' \equiv \pm 1(8) \text{ und } \beta' \equiv 3(8))$ oder $(\alpha' \equiv \pm 3(8) \text{ und } \beta' \equiv \pm 1(8)) \Rightarrow (\alpha'^2 \equiv 1(16) \text{ und } \beta'^2 \equiv 9(16))$ oder $(\alpha'^2 \equiv 9(16) \text{ und } \beta'^2 \equiv 1(16))$. Durch Einsetzen in (i) ergibt dies wieder in beiden Fällen $-2 \equiv 6(16)$.

LITERATUR

- [1] Anderson, D.F.: Projective modules over subrings of $k[X, Y]$, Trans. Amer. Math. Soc. 240(1978), 317 - 328
- [2] Artin, M.: Grothendieck Topologies, Harvard University, Cambridge, Mass. 1962
- [3] Auslander, M.; Goldman, O.: The Brauer group of a commutative ring, Trans. Amer. Math. Soc. 97 (1960), 367 - 409
- [4] Baeza, R.: Quadratic Forms Over Semilocal Rings, Lecture Notes 655, Springer - Verlag, Berlin - Heidelberg - New York 1978
- [5] Bass, H.: Lectures on Topics in Algebraic K-Theory, Tata Institute of Fundamental Research, Bombay, 1967
- [6] Bass, H.: Algebraic K-Theory, Benjamin, New York 1968
- [7] Bass, H.: Clifford algebras and Spinor norms over a commutative ring, Amer. J. Math. 96 (1974), 156 - 206
- [8] Borevič, Z. I. ; Šafarevič, I.R.: Zahlentheorie, Birkhäuser, Stuttgart, 1966
- [9] Bourbaki, N.: Algèbre Chap. 9, Formes sesquilineaires et formes quadratiques, Hermann, Paris, 1959
- [10] Bourbaki, N.: Algèbre Commutative Chap. 1-2, Hermann, Paris, 1961
- [11] Bourbaki, N.: Algèbre Chap. 1-3, Hermann, Paris, 1970

- [12] Chase, S.U.; Harrison D.K.; Rosenberg, A.: Galois theory and Galois cohomology of commutative rings, Mem. Amer.Math. Soc. 52 (1965), 15-33
- [13] Chase, S.U.; Rosenberg, A.: Amitsur cohomology and the Brauer group, Mem. Amer. Math. Soc. 52 (1965), 34-79
- [14] Childs, L.N.: Abelian Galois extensions of rings containing roots of unity, Illinois J. Math. 15 (1971), 273-280
- [15] Childs, L.N.: The group of unramified Kummer extensions of prime degree, Proc. London Math. Soc. 35 (1977), 407 - 422
- [16] Childs, L.N.; Magid A.: The Picard invariant of a principal homogeneous space, J. Pure Appl. Algebra 4 (1974), 273 - 286
- [17] DeMeyer, F.; Ingraham E.: Separable algebras over commutative rings, Lecture Notes 181, Springer-Verlag, Berlin - Heidelberg - New York, 1971
- [18] Fossum, R.M.: The divisor class group of a Krull domain, Ergebnisse der Mathematik 74, Springer-Verlag, Berlin u.a., 1970
- [19] Fröhlich, A.: Discriminants of algebraic number fields, Math. Zeitschr. 74 (1960), 18 - 28
- [20] Fröhlich, A.: The discriminants of relative extensions and the existence of integral bases, Mathematika 7 (1960), 15 - 22
- [21] Fröhlich, A.: Discriminants and module invariants over a Dedekind domain, Mathematika 8 (1961), 170-172

- [22] Fröhlich, A.: Ideals in an extension field as modules over the algebraic integers in a finite number field, Math. Z. 74 (1960), 29 - 38
- [23] Garfinkel, G.; Orzech, M.: Galois extensions as modules over the group ring, Canad. J. Math. 22 (1970), 242 - 248
- [24] Grothendieck, A.: Technique de descente I, Séminaire Bourbaki, Exposé 190 (1959 - 1960)
- [25] Grothendieck, A.: Sur quelques points d'algèbres homologique, Tôhoku Math. J. 9 (1957), 119 - 221
- [26] Harrison, D.: Abelian extensions of commutative rings, Mem. Amer. Math. Soc. 52 (1965), 1 - 14
- [27] Kanzaki, T.: On the quadratic extensions and the extended Witt ring of a commutative ring, Nagoya Math. J. 49 (1973), 127 - 141
- [28] Kitamura, K.: On the free quadratic extensions of a commutative ring, Osaka J. Math. 10 (1973), 15 - 20
- [29] Knus, M.A.; Ojanguren, M.: Théorie de la descente et Algebres d'Azumaya, Lecture Notes 383, Springer-Verlag, Berlin u.a., 1974
- [30] Maurer, D.: Invariants of the Trace-form of a Number field, Lin. multilin. Alg. 6 (1978), 33 - 36
- [31] Micali, A.; Villamayor, O.E.: Sur les algèbres de Clifford I, Ann. scient. Éc. Norm. Sup., 4^e série, 1 (1968), 271 - 304
- [32] Micali, A.; Villamayor, O.E.: Sur les algèbres de Clifford II, J. Reine angew. Math. 242 (1970), 61-90

- [33] Micali, A.; Villamayor, O.E.: Algèbres de Clifford et groupe de Brauer, Ann. scient. Éc. Norm. Sup., 4^e série, 4 (1971), 285 - 310
- [34] Narkiewicz, W.: Elementary and analytic theory of algebraic numbers, PWN, Warszawa, 1973
- [35] Orzech, M.: A cohomological description of abelian Galois extensions, Trans. Amer. Math. Soc. 137 (1969), 481 - 499
- [36] Revoy, P.: Sur les deux premiers invariants d'une forme quadratique, Ann. scient. Éc. Norm. Sup., 4^e série, 4 (1971), 311 - 319
- [37] Small, C.: The Brauer-Wall group of a commutative ring, Trans. Amer. Math. Soc. 156 (1971), 455 - 491
- [38] Small, C.: The group of quadratic extensions, J. Pure Appl. Alg. 2 (1972), 83 - 105 and 395
- [39] Small, C.: Normal bases for quadratic extensions, Pac. J. Math. 50 (1974), 601 - 611
- [40] Thérond, J.-D.: Sur deux conjectures de Small, Bull. Soc. Math. France 48(1976), 117-122
- [41] Thérond, J.-D.: Le groupe des extensions quadratiques séparables libres de l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$, C.R. Acad. Sc. Paris, 281 (1975), Série A, 939 - 942
- [42] Villamayor, O.E.; Zelinsky, D.: Galois theory for rings with finitely many idempotents, Nagoya Math. J. 27 (1966), 721 - 731

Lebenslauf

- 12.6.1950 geboren in Neuburg/Ka.
- 1956-1969 Besuch der Volksschule und des Simpert-Kraemer-Gymnasiums in Krumbach; Abitur
- 1969-1975 Studium der Mathematik an der Universität München; Diplom in Mathematik
- 1973-1975 wissenschaftliche Hilfskraft am Mathematischen Institut der Universität München
- 1975-1976 Studium an der Universität Zürich; Diplom für das höhere Lehramt im Kanton Zürich (1
- seit 1976 Verwalter der Dienstgeschäfte eines wissenschaftlichen Assistenten am Mathematischen Institut der Universität München

